Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004099

International filing date: 09 March 2005 (09.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-106946
Filing date: 31 March 2004 (31.03.2004)

Date of receipt at the International Bureau: 20 May 2005 (20.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)

PCT/JP2005/004099
19.04.2005

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

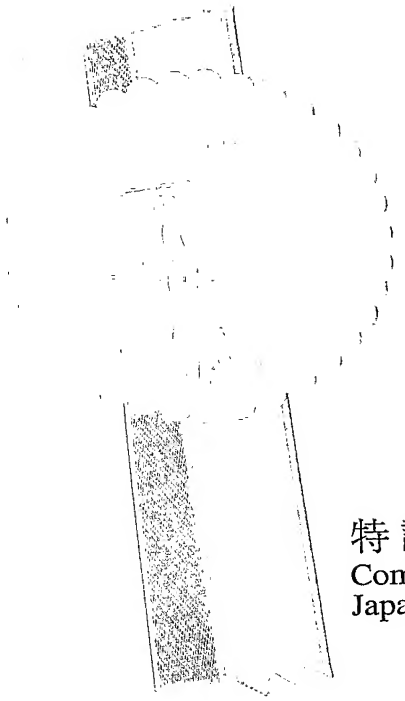
This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００４年　３月３１日

出願番号
Application Number: 特願２００４－１０６９４６

[ST. 10/C]: ［ＪＰ２００４－１０６９４６］

出願人
Applicant(s): オムロン株式会社



２００５年　３月１１日

特許庁長官
Commissioner,
Japan Patent Office

小川洋

出証番号　出証特２００５－３０２１３３８

【書類名】　特許願
【整理番号】　62851
【提出日】　平成16年 3月31日
【あて先】　特許庁長官　殿
【国際特許分類】　B60R 25/00　606
B60R 25/04　602
B60R 25/04　608
【発明者】
【住所又は居所】　京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内
【氏名】　安藤　丹一
【発明者】
【住所又は居所】　京都府京都市下京区塩小路通堀川東入南不動堂町８０１番地　オムロン株式会社内
【氏名】　竹内　寿
【特許出願人】
【識別番号】　000002945
【氏名又は名称】　オムロン株式会社
【代理人】
【識別番号】　100080034
【弁理士】
【氏名又は名称】　原　謙三
【電話番号】　06-6351-4384
【手数料の表示】
【予納台帳番号】　003229
【納付金額】　21,000円
【提出物件の目録】
【物件名】　特許請求の範囲　1
【物件名】　明細書　1
【物件名】　図面　1
【物件名】　要約書　1
【包括委任状番号】　0101830

【書類名】特許請求の範囲
【請求項１】
情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置であって、
複数の上記情報送受信装置それぞれと通信を行う通信装置と、
上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識装置と、
上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶装置と、
上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定手段と、
上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第１警戒指示手段と、
上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第２警戒指示手段と、
上記位置履歴情報に基づいて、上記第１警戒指示手段による指示、および第２警戒指示手段による指示のうちいずれかの指示を選択する警戒状態選択手段とを備えていることを特徴とする情報処理装置。
【請求項２】
上記所定領域内への人の出入りを検知する人行動監視手段をさらに備え、
上記警戒状態選択手段が、上記位置履歴情報に加えて、上記人行動監視手段による検知結果に基づいて指示の選択を行うことを特徴とする請求項１に記載の情報処理装置。
【請求項３】
上記警戒状態選択手段は、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域内から所定領域外に移動する情報送受信装置とがあると判定した場合、上記第１警戒指示手段の指示を選択し、
上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域外から所定領域内に移動する情報送受信装置とがあると判定した場合、上記第２警戒指示手段の指示を選択することを特徴とする請求項２に記載の情報処理装置。
【請求項４】
上記警戒状態選択手段が、情報送受信装置に対して、該情報送受信装置の利用者による入力応答を要求する応答要求手段を備えており、
上記位置履歴情報に基づき、上記所定領域内に情報送受信装置が所定期間ある場合、
上記応答要求手段が上記所定領域内にある情報送受信装置に対して上記入力応答を要求し、
上記入力応答の返信がない場合に、
上記警戒状態選択手段は、上記所定領域内に所定期間存在する情報送受信装置と、所定領域内から所定領域外に移動する情報送受信装置とがあると判定した場合、上記第１警戒状態手段の指示を選択し、
上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域外から所定領域内に移動する情報送受信装置とがあると判定した場合、上記第２警戒指示手段の指示を選択することを特徴とする請求項２に記載の情報処理装置。
【請求項５】
上記警戒状態選択手段によって選択された上記指示に関する情報を、上記複数の情報送受信装置それぞれに対して上記通信装置を介して通知する警戒状態通知手段をさらに備えていることを特徴とする請求項１～４に記載の情報処理装置。
【請求項６】
上記請求項１～５に記載の情報処理装置と、当該情報処理装置と通信をする情報送受信装置とを備える情報処理制御システム。
【請求項７】
情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置の制御方法であって、

複数の上記情報送受信装置それぞれと通信を行う通信ステップと、
上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識ステップと、
上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶ステップと、
上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定ステップと、
上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第１警戒指示ステップと、
上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第２警戒指示ステップと、
上記位置履歴情報に基づいて、上記第１警戒指示ステップによる指示、および第２警戒指示ステップによる指示のうちいずれかを選択する警戒状態選択ステップとを含むことを特徴とする情報処理装置の制御方法。
【請求項８】
請求項１～５の何れか１項に記載の情報処理装置を動作させるための制御プログラムであって、コンピュータを上記各手段として機能させるための情報処理装置の制御プログラム。
【請求項９】
請求項８に記載の情報処理装置の制御プログラムが記録されたコンピュータの読取り可能な記録媒体。

【書類名】明細書
【発明の名称】情報処理装置、情報処理制御システム、情報処理装置の制御方法、情報処理装置の制御プログラム、情報処理装置の制御プログラムを記録した記録媒体
【技術分野】
【０００１】
本発明は、情報送受信装置を携帯した人が所定領域内から所定領域外に移動する場合に警戒状態とし、該情報送受信装置を携帯した人が所定領域外から所定領域内に移動した場合に警戒状態を解除する情報処理装置に関するものである。
【背景技術】
【０００２】
近年、車上荒らしや住居への不法侵入等の様々な犯罪が多発化しており、人々の防犯意識が高まっている。そして、この防犯意識の高まりを受け、様々な防犯用商品が開発されている。
【０００３】
例えば、電波を利用した車両用のセキュリティ機構制御システムの一態様として、車両のドア錠の解錠／施錠を行うセキュリティ機構制御システムがある。このセキュリティ機構制御システムでは、ユーザが携帯器を持ち歩くだけで自動的に解錠／施錠が行われ、施錠されていることを容易にこの利用者が確認できるものである（例えば特許文献１～３参照）。このセキュリティ機構制御システムでは、携帯器が信号を送出し、親機がこの信号を受信するようになっており、ユーザがこの携帯器を所持し、車両に近づくだけで自動的に解錠され、逆に車両から離れると施錠されるように構成されている。
【特許文献１】特開２００３－２７７９０号公報（公開日２００３年１月２９日）
【特許文献２】特開２００３－２７７９１号公報（公開日２００３年１月２９日）
【特許文献３】特開２００３－３０１６３８号公報（公開日２００３年１０月２４日）
【発明の開示】
【発明が解決しようとする課題】
【０００４】
ところで、従来のように携帯器を持った利用者の乗降に応じて、自動的に車両のドア錠の解錠／施錠を行うシステムにおいて、セキュリティ管理対象が車両のように複数のユーザによって利用されるものである場合、この携帯器を複数用意しそれぞれを利用可能とする制御システムが考えられる。
【０００５】
ところが、複数の携帯器を利用可能とした場合、複数ある携帯器のうちいずれかを車内に置き忘れる可能性が高くなる。このように、複数ある携帯器のうち車内に置き忘れられた携帯器がある場合、従来の構成では次の問題が生じる。
【０００６】
つまり、置き忘れた携帯器が車内にあるため、親機が、この携帯器の所有者であるユーザが車内にいると判断し、車両を警戒状態に自動設定しない場合がある。この場合は、携帯器を車内に置き忘れたことにユーザが気付かないまま、車を非警戒状態のままにしてしまうという問題が生じる。
【０００７】
また、複数のユーザいずれもが携帯器を所持しており、その複数ユーザのいずれかの降車に応じて、自動的に車両の施錠が行われるように設定される場合、あるいは、車に対して直接、ユーザが施錠をするように指示する場合がある。
【０００８】
この両者のいずれの場合であっても、車内に置き忘れられた携帯器がある場合、ユーザ以外の人がこの車に接近すると、自動的に解錠されてしまうという問題が生じる。これは、上記車に対して近づく人がおり、かつ親機の近くに携帯器があるという条件を満たすために、上記車に設定した施錠状態が自動的に解錠されてしまうからである。

【０００９】
また、複数の携帯器が利用可能なシステムの場合、ある人は携帯器をもって親機から離れていくがある人は、親機近辺にいるといった状態も起こり得る。
【００１０】
この場合、前者の人は、自動的に車に施錠がされたと認識しているが、後者の人が親機のそばにいるため施錠されないこととなる。すなわち、各ユーザの挙動に左右され、一方では施錠する条件を満たしているにもかかわらず、他方では解錠する条件を満たしており、上記の場合は、親機が解錠する条件を選択した結果である。
【００１１】
したがって、複数の携帯器が利用可能な場合にはユーザが所望する状態に親機が必ずしも設定しないという問題が生じる。
【００１２】
上記特許文献１～３での構成では、親機の近辺に置き忘れられた携帯器またはユーザが所持している携帯器が存在する場合、親機の近辺にある携帯器が置き忘れられた携帯器であるのか、ユーザが所持している携帯機であるのかを区別する手段と、この区別した結果に応じてユーザに適切に通知する手段とがないため、上記した問題には対処することができないこととなる。
【００１３】
したがって、携帯器を複数利用可能とした場合、上記特許文献１～３の構成では、ユーザが知らない間に、ユーザの意図に反して車に施錠がされない、または施錠した状態から解除されるという問題が生じる。
【００１４】
本発明は、上記の問題点に鑑みてなされたものであり、その目的は、複数の情報送受信装置が情報処理装置に登録されている場合、当該複数の情報送受信装置の置き忘れによって生じる警戒状態の設定の誤操作を解消することを実現することにある。
【課題を解決するための手段】
【００１５】
本発明に係る情報処理装置は、上記課題を解決するために、情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置であって、複数の上記情報送受信装置それぞれと通信を行う通信装置と、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識装置と、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶装置と、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定手段と、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第１警戒指示手段と、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第２警戒指示手段と、上記位置履歴情報に基づいて、上記第１警戒指示手段による指示、および第２警戒指示手段による指示のうちいずれかの指示を選択する警戒状態選択手段とを備えていることを特徴とする。
【００１６】
上記警戒状態とは、所定の利用者以外が所定の領域に接近することに対して例えば、警告、威嚇、または施錠などの阻害行為を行うよう設定された状態である。そして、本発明に係る情報処理装置は情報送受信装置を携帯した人が所定領域内にいるか否かに応じてこの警戒状態の設定を切り替えるものであり、また当該情報送受信装置とは通信部によって通信可能になっている。
【００１７】
この情報処理装置は、位置認識装置と位置判定手段を備えているため、情報送受信装置それぞれの位置を把握することができ、情報送受信装置それぞれが所定領域内に存在するか否かを判定することができる。
【００１８】

また、情報処理装置は、履歴記憶装置を備えているため、各情報送受信装置の動きを知ることができ、情報送受信装置が所定領域内から所定領域外に移動したのか、所定領域外から所定領域内に移動したのか、あるいは所定領域内の一定の位置に留まっているのかを知ることができる。

【００１９】

また、情報処理装置は、第１警戒指示手段を備えているため、位置履歴情報、すなわち情報処理装置が所定領域内に存在しているのか否かと、所定領域内に入ってきた、または所定領域内から出ていったものであるのか、所定領域内の一定の位置に留まっているのかというの情報に基づき、自動的に警戒状態または非警戒状態に切り替えるのか、あるいはユーザの入力指示に応じて警戒または非警戒に切り替えるのかを決定することができる。

【００２０】

したがって、上記情報処理装置は、例えば、情報送受信装置が所定領域内に置き忘れられた場合、他の情報送受信装置が所定領域内に入ってきた際に自動的に非警戒にするのか、常に警戒にするのか、あるいは、所定領域内に入ってきた情報送受信装置に対して通知を行い、情報送受信装置からの指示に応じて、警戒または非警戒を決定するのか選択することができる。

【００２１】

それ故、上記情報処理装置は、各情報送受信装置の位置関係と、所定期間での各情報送受信装置の挙動とによって適切に警戒状態の設定または解除を自動で行うのかあるいは情報送受信装置からの指示に基づき行うのかを決定することができる。

【００２２】

また、本発明に係る情報処理装置は、上記構成において、上記所定領域内への人の出入りを検知する人行動監視手段をさらに備え、上記警戒状態選択手段が、上記位置履歴情報に加えて、上記人行動監視手段による検知結果に基づいて指示の選択を行う構成であってもよい。

【００２３】

これにより、情報処理装置は、人行動監視手段を備えているため、携帯の位置だけでなく、ユーザの位置および挙動も検知することができる。このため、情報送受信装置を携帯する利用者の位置および挙動を精度良く把握することができる。

【００２４】

また、本発明に係る情報処理装置は、上記構成において、上記警戒状態選択手段が、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送信装置と、所定領域内から所定領域外に移動する情報送信装置とがあると判定した場合、上記第１警戒指示手段の指示を選択し、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送信装置と、所定領域外から所定領域内に移動する情報送信装置とがあると判定した場合、上記第２警戒指示手段の指示を選択する構成であってもよい。

【００２５】

すなわち、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置がある場合これを利用者によって所持されていない情報送受信装置であると特定することができる。

【００２６】

また、所定領域内において所定期間、情報送受信装置が有る場合、他の情報送受信装置が所定領域から出て行くときに、所定領域を警戒状態とすることができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有るために警戒状態とならず、警戒状態が解除された状態のままとなることを防ぐことができる。

【００２７】

また、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置がある場合、他方の情報送受信装置が所定領域に入ってくるときに、警戒状態である所定領域の警戒を第２警戒指示手段の指示、すなわちユーザの入力指示に基づき、解除することができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有り、

情報送受信装置を所持しない人が所定領域内に入ってきたため、置き忘れられた情報送受信装置と、情報送受信装置を所持していない人との組み合わせを、携帯を所持する正規のユーザと誤って、警戒状態の解除を行うことを防ぐことができる。

【００２８】

本発明に係る情報処理装置は、上記構成において、上記警戒状態選択手段が、上記警戒状態選択手段が、情報送受信装置に対して、該情報送受信装置の利用者による入力応答を要求する応答要求手段を備えており、上記位置履歴情報に基づき、上記所定領域内に情報送受信装置が所定期間ある場合、上記応答要求手段が上記所定領域内にある情報送受信装置に対して上記入力応答を要求し、上記入力応答の返信がない場合に、上記警戒状態選択手段は、上記所定領域内に所定期間存在する情報送受信装置と、所定領域内から所定領域外に移動する情報送受信装置とがあると判定した場合、上記第１警戒状態手段の指示を選択し、上記位置履歴情報に基づき、上記所定領域内に所定期間存在する情報送受信装置と、所定領域外から所定領域内に移動する情報送受信装置とがあると判定した場合、上記第２警戒指示手段の指示を選択する構成であってもよい。

【００２９】

すなわち、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置に対して、さらに入力応答を要求することによって、所定領域内にある情報処理装置が利用者によって携帯されている情報送受信装置であるのか否かを精度良く判定することができる。

【００３０】

また、この利用者が携帯していない情報送受信装置が所定領域内にあると判定した場合において、他の情報送受信装置が所定領域から出て行くときに、所定領域を警戒状態とすることができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有るために警戒状態とならず、警戒状態が解除された状態のままとなることを防ぐことができる。

【００３１】

また、上記情報処理装置は、所定領域に所定期間存在する情報送受信装置がある場合、他方の情報送受信装置が所定領域に入ってくるときに、警戒状態である所定領域の警戒を第２警戒指示手段の指示、すなわち利用者の入力指示に基づき、解除することができる。このため、情報処理装置は、例えば所定領域内に置き忘れられた情報送受信装置が有り、情報送受信装置を所持しない人が所定領域内に入ってきたため、置き忘れられた情報送受信装置と、情報送受信装置を所持していない人との組み合わせを、携帯を所持する正規のユーザと誤って、警戒状態の解除を行うことを防ぐことができる。

【００３２】

また、本発明に係る情報処理装置は、上記した構成において、上記警戒状態選択手段によって選択された上記指示に関する情報を、上記複数の情報送受信装置それぞれに対して上記通信装置を介して通知する警戒状態通知手段をさらに備えていてもよい。

【００３３】

すなわち、上記情報処理装置は、警戒状態通知手段を備えているため、所定領域内に設定される警戒状態がどの状態であるのかをユーザは知ることができる。

【００３４】

したがって、情報処理装置によって設定された警戒状態が適切なものであるのか否かを情報送受信装置を介してユーザは知ることができ、不適切な設定である場合は、ユーザはこの設定を変更するように指示を出すことができる。

【００３５】

よって、上記情報処理装置は、ユーザの意思を反映させて警戒状態の設定または解除を設定することができる。

【００３６】

また、本発明に係る情報処理制御システムは、上記した情報処理装置と、当該情報処理装置と通信をする情報送受信装置とを備える情報処理制御システムである。

【００３７】

また、本発明に係る情報処理装置の制御方法は、情報送受信装置を携帯した利用者の所定領域に対する出入りを監視し、所定領域に対する警戒動作の制御を行う情報処理装置の制御方法であって、複数の上記情報送受信装置それぞれと通信を行う通信ステップと、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識ステップと、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶ステップと、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定ステップと、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第１警戒指示ステップと、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第２警戒指示ステップと、上記位置履歴情報に基づいて、上記第１警戒指示ステップによる指示、および第２警戒指示ステップによる指示のうちいずれかを選択する警戒状態選択ステップとを含むことを特徴とする。

【００３８】

なお、上記情報処理装置は、コンピュータによって実現してもよく、この場合には、コンピュータを上記各手段として動作させることにより上記情報処理装置をコンピュータにて実現させる情報処理装置の制御プログラムを記録したコンピュータ読取り可能な記録媒体も、本発明の範疇に入る。

【発明の効果】

【００３９】

本発明に係る情報処理装置は、以上のように、複数の上記情報送受信装置それぞれと通信を行う通信装置と、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識装置と、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶装置と、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定手段と、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第１警戒指示手段と、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第２警戒指示手段と、上記位置履歴情報に基づいて、上記第１警戒指示手段による指示、および第２警戒指示手段による指示のうちいずれかの指示を選択する警戒状態選択手段とを備えている。

【００４０】

また、本発明に係る情報処理装置の制御方法は、以上のように、複数の上記情報送受信装置それぞれと通信を行う通信ステップと、上記複数の情報送受信装置それぞれの位置を示す位置情報を取得する位置認識ステップと、上記位置情報の所定期間の履歴である位置履歴情報を記憶する履歴記憶ステップと、上記位置情報に基づき、上記情報送受信装置のそれぞれが所定領域内にあるか否かを判定する位置判定ステップと、上記位置判定手段の判定結果に応じて、警戒状態の設定または解除を指示する第１警戒指示ステップと、上記情報送受信装置から警戒状態の設定または解除を指示する要求情報を上記通信装置を介して受信し、警戒状態の設定または解除を指示する第２警戒指示ステップと、上記位置履歴情報に基づいて、上記第１警戒指示ステップによる指示、および第２警戒指示ステップによる指示のうちいずれかを選択する警戒状態選択ステップとを含んでいる。

【００４１】

このため、上記情報処理装置は、各情報送受信装置の位置関係と、所定期間での各情報送受信装置の挙動とによって適切に警戒状態の設定または解除を自動で行うのかあるいは情報送受信装置からの指示に基づき行うのかを決定することができるという効果を奏する。

【発明を実施するための最良の形態】

【００４２】

本実施の形態に係るカーセキュリティシステム１は、セキュリティ装置２と、このセキュリティ装置２に登録されたセキュリティコントローラ３ａ～３ｃとによって構成されるシステムである。そしてこのシステム１は、正規ユーザ以外の人が警戒状態に設定されて

いる車のドアを開閉するなどの異常状態に対し、威嚇を行う防犯システムである。

【００４３】

なお、車に対する上記異常状態は、例えば、正規ユーザ以外の人が車のトランクを開けようとする行為，フロントガラス等の破壊行為，ジャッキアップなどによって車のタイヤを取り外そうとする行為に伴う振動等として検知される。

【００４４】

具体的には、図２および図３に示すように本実施の形態に係るセキュリティシステム１では、セキュリティ装置２が所定の範囲にわたるセキュリティ管理領域５０という領域を設定している。図２は、セキュリティ管理領域５０における、セキュリティコントローラ３を携帯した人（ユーザ）と、セキュリティコントローラ３を携帯しない人との関係を示す図である。図３は、セキュリティ管理対象である車５１を含むセキュリティ管理領域５０における、セキュリティコントローラ３を携帯した人（ユーザ）と、セキュリティコントローラ３を携帯しない人との関係を示す図である。

【００４５】

このセキュリティ管理領域５０とは、当該領域への人の出入りが制限され不正に領域内の管理対象物を利用されないように管理された領域である。例えば、駐車中の車，家屋，敷地，ビル，オフィス，店舗，作業場所，作業机などのセキュリティ管理対象に対して、不正利用や不正侵入等が行われることを防ぐことが求められる領域である。

【００４６】

具体的には、図３に示すように、このセキュリティシステム１では、セキュリティコントローラ３を所持するユーザが、このセキュリティ管理領域５０内からセキュリティ管理領域５０外に出て行くと警戒状態に自動的に設定される。一方、セキュリティシステム１では、上記ユーザがセキュリティ管理領域５０外からセキュリティ管理対象である車５１に近づくと警戒設定が自動的に解除されるように設定されている。

【００４７】

なお、本明細書においてオートセキュリティ機能とは、セキュリティコントローラ３を保持した正規ユーザが、車５１から降車し上記セキュリティ管理領域５０外に移動すると自動的に車に警戒状態の設定を行い、逆にセキュリティ管理領域５０内にこのユーザが入ると自動的に車に設定されている警戒状態の設定を解除する機能のこととする。

【００４８】

また、上記セキュリティ管理領域５０の範囲としては、警戒設定対象である車を中心に半径５メートル以内であることが好ましいがこれに限定されるものではない。セキュリティ装置２は、繁華街等、人の往来が激しい地域では、上記した半径５メートルの範囲よりも狭い範囲に上記セキュリティ管理領域５０が設定可能となる構成であることが好ましい。

【００４９】

また、車に対するこの警戒状態の設定および解除は、正規のユーザが直接所持するセキュリティコントローラ３ａ～３ｃによってセキュリティ装置２に指示を出すことで設定を切り替えることもできる。

【００５０】

次に、上記したセキュリティシステム１の概略構成について図４を参照して説明する。

【００５１】

本実施の形態に係るセキュリティシステム１は、車に搭載されるセキュリティ装置２と、このセキュリティ装置１に対して通信可能となるように登録された３つのセキュリティコントローラ３ａ～３ｃを備えている。そして、このセキュリティ装置２とセキュリティコントローラ３ａ～３ｃとは、無線によって相互に通信可能となっている。また、セキュリティコントローラ３ａ～３ｃ同士も互いに無線によって通信可能となっている。

【００５２】

なお、本明細書において特にセキュリティコントローラ３ａ～３ｃを区別する必要がない場合には、セキュリティコントローラ３と表記する。

【００５３】
次に、本実施の形態に係るセキュリティ装置２の概略構成について図１を参照して説明する。図１は、セキュリティ装置２の概略構成の一例を示すブロック図である。

【００５４】
本実施の形態に係るセキュリティ装置２は、ＡＣＣ検出部６，接近物検出部７，通信部４，威嚇部５，異常検出部８，記憶部１１，およびセキュリティ管理処理部１０を備えている。そして、セキュリティ装置２は、車内のアクセサリー電源（以下ＡＣＣと称する）とＡＣＣ検出部６を介して接続されている。

【００５５】
このＡＣＣ検出部６は、セキュリティ装置２が接続されているＡＣＣの電源供給が「オン」または「オフ」であるのかを検出するものである。すなわち、車が停車しキーがはずされるとＡＣＣの電源は「オン」から「オフ」に切り換わる。このため、ＡＣＣ検出部６がＡＣＣの電源が「オフ」であると検出した場合、車のエンジンが切られ車は停止状態にあることを示す。逆に、ＡＣＣ電源検出部６がＡＣＣの電源が「オン」であると検出した場合、車が始動中であることを示す。

【００５６】
このＡＣＣ検出部６は、検出したＡＣＣ電源の「オン」または「オフ」の情報をセキュリティ管理処理部１０に送信する。

【００５７】
接近物検出部７は、セキュリティシステム１のセキュリティ管理対象である車に接近してくる、例えば人などの対象物を検出するものである。この接近物検出部７は、マイクロ波を利用したドップラー効果によって車両周辺の移動物を検知する、いわゆるドップラセンサによって実現できる。この接近物検出部７は、車に接近する対象物、すなわち上記セキュリティ管理領域５０内に侵入する人を検出するとその情報をセキュリティ管理処理部１０に送信する。

【００５８】
異常検出部８は、セキュリティシステム１のセキュリティ管理対象である車に対して、この車の外部から与えられた振動等の異常を検出するものである。この異常とは、例えば、正規のユーザ以外の人が車のドアを開けようとし生じる振動や、車のガラスの破壊によって生じる振動、車を移動させるためにジャッキアップされることによって生じる車の傾きなどである。異常検出部８は、上記異常を検出した場合、この検出した情報を威嚇部５に通知する。

【００５９】
通信部４は、セキュリティ管理処理部１０の指示に応じて、上記セキュリティコントローラ３ａ～３ｃそれぞれと互いに通信を行うものである。この通信部４は、例えばＰＩＮＧコマンド等の制御信号をセキュリティコントローラ３ａ～３ｃそれぞれに送信したり、セキュリティコントローラ３ａ～３ｃそれぞれから送信された警戒設定および／または警戒設定解除等を指示するコマンドを受信したりすることができる。なお、後述するが、通信部４は、セキュリティコントローラ３ａ～３ｃそれぞれの所在位置を確認するために、当該セキュリティコントローラ３ａ～３ｃから送られる電波を受信するように構成されており、受信したこの電波の情報をセキュリティ管理処理部１０に送信する。また、セキュリティコントローラ３ａ～３ｃからコマンドを受信した場合も同様にセキュリティ管理処理部１０に送信する。

【００６０】
威嚇部５は、車が警戒（警戒モード）に設定されている際に、上記異常検出部８がセキュリティシステム１のセキュリティ管理対象である車において異常を検出した場合、警報音を発生させたり、発光させたりして車に接近し不法行為を行おうとする正規ユーザ以外の人に対して威嚇を行うものである。

【００６１】
なお、異常が検出された場合に、威嚇部５によって威嚇が行われるとともに、例えば携

帯電話通信網などを利用して、異常が検出されたことを示す情報を、警備サービスを提供するセキュリティセンタに通報することが可能となっていてもよい。

【００６２】

上記セキュリティ管理処理部１０は、上記したセキュリティ装置２が備える各部材に対する各種制御を行うものである。このセキュリティ管理処理部１０の詳細な説明は後述する。

【００６３】

記憶部１１は、読み書き可能な不揮発性の記憶媒体であり、セキュリティ管理処理部１０が各種処理を行うにあたり必要となる情報を記録したり、記録された情報を参照したりするものである。この記憶部１１に記録される情報の詳細な説明は後述する。

【００６４】

なお、図４に示す各機能ブロックは、通信部４，威嚇部５，ＡＣＣ検出部６，接近物検出部７，および異常検出部８の各部材とＣＰＵ（central processing unit）と，ＲＡＭ（random access memory）と，ＲＯＭ（read only memory）とがそれぞれバスを介して接続されており、ＣＰＵがＲＯＭに記憶されたプログラムをＲＡＭに読出しプログラムを実行することで実現できる。

【００６５】

また、セキュリティ装置２が備える記憶部１１は、例えばフラッシュＥＥＰＲＯＭなどの不揮発性記憶媒体によって実現可能である。

【００６６】

なお、上記では、各機能ブロックが「ＣＰＵなどの演算手段がＲＯＭやＲＡＭなどの記録媒体に格納されたプログラムコードを実行することで実現される」場合を例にして説明したが、同様の処理を行うハードウェアで実現してもよい。また、処理の一部を行うハードウェアと、当該ハードウェアの制御や残余の処理を行うプログラムコードを実行する上記演算手段とを組み合わせても実現することもできる。さらに、上記各部材のうち、ハードウェアとして説明した部材であっても、処理の一部を行うハードウェアと、当該ハードウェアの制御や残余の処理を行うプログラムコードを実行する上記演算手段とを組み合わせても実現することもできる。なお、上記演算手段は、単体であってもよいし、装置内部のバスや種々の通信路を介して接続された複数の演算手段が共同してプログラムコードを実行してもよい。

【００６７】

上記演算手段によって直接実行可能なプログラムコード自体、または、後述する解凍などの処理によってプログラムコードを生成可能なデータとしてのプログラムは、当該プログラム（プログラムコードまたは上記データ）を記録媒体に格納し、当該記録媒体を配付したり、あるいは、上記プログラムを、有線または無線の通信路を介して伝送するための通信装置で送信したりして配付され、上記演算手段で実行される。

【００６８】

なお、例えばバスなどの通信路を介して伝送する場合、通信路を構成する各伝送媒体が、プログラムを示す信号列を伝搬し合うことによって、当該通信路を介して、上記プログラムが伝送される。また、信号列を伝送する際、送信装置が、プログラムを示す信号列により搬送波を変調することによって、上記信号列を搬送波に重畳してもよい。この場合、受信装置が搬送波を復調することによって信号列が復元される。一方、上記信号列を伝送する際、送信装置が、デジタルデータ列としての信号列をパケット分割して伝送してもよい。この場合、受信装置は、受信したパケット群を連結して、上記信号列を復元する。また、送信装置が、信号列を送信する際、時分割／周波数分割／符号分割などの方法で、信号列を他の信号列と多重化して伝送してもよい。この場合、受信装置は、多重化された信号列から、個々の信号列を抽出して復元する。いずれの場合であっても、通信路を介してプログラムを伝送できれば、同様の効果が得られる。

【００６９】

ここで、プログラムを配付する際の記録媒体は、取外し可能である方が好ましいが、プ

ログラムを配付した後の記録媒体は、取外し可能か否かを問わない。また、上記記録媒体は、プログラムが記憶されていれば、書換え（書き込み）可能か否か、揮発性か否か、記録方法および形状を問わない。記録媒体の一例として、磁気テープやカセットテープなどのテープ、あるいは、フロッピー（登録商標）ディスクやハードディスクなどの磁気ディスク、または、ＣＤ－ＲＯＭや光磁気ディスク（ＭＯ）、ミニディスク（ＭＤ）やデジタルビデオディスク（ＤＶＤ）などのディスクが挙げられる。また、記録媒体は、ＩＣカードや光カードのようなカード、あるいは、マスクＲＯＭやＥＰＲＯＭ、ＥＥＰＲＯＭまたはフラッシュＲＯＭなどのような半導体メモリであってもよい。あるいは、ＣＰＵなどの演算手段内に形成されたメモリであってもよい。

【００７０】

なお、上記プログラムコードは、上記各処理の全手順を上記演算手段へ指示するコードであってもよいし、所定の手順で呼び出すことで、上記各処理の一部または全部を実行可能な基本プログラム（例えば、オペレーティングシステムやライブラリなど）が既に存在していれば、当該基本プログラムの呼び出しを上記演算手段へ指示するコードやポインタなどで、上記全手順の一部または全部を置き換えてもよい。

【００７１】

また、上記記録媒体にプログラムを格納する際の形式は、例えば、実メモリに配置した状態のように、演算手段がアクセスして実行可能な格納形式であってもよいし、実メモリに配置する前で、演算手段が常時アクセス可能なローカルな記録媒体（例えば、実メモリやハードディスクなど）にインストールした後の格納形式、あるいは、ネットワークや搬送可能な記録媒体などから上記ローカルな記録媒体にインストールする前の格納形式などであってもよい。また、プログラムは、コンパイル後のオブジェクトコードに限るものではなく、ソースコードや、インタプリトまたはコンパイルの途中で生成される中間コードとして格納されていてもよい。いずれの場合であっても、圧縮された情報の解凍、符号化された情報の復号、インタプリト、コンパイル、リンク、または、実メモリへの配置などの処理、あるいは、各処理の組み合わせによって、上記演算手段が実行可能な形式に変換可能であれば、プログラムを記録媒体に格納する際の形式に拘わらず、同様の効果を得ることができる。

【００７２】

（セキュリティ管理処理部の構成）

次に、セキュリティ管理処理部１０の概略構成について説明する。

【００７３】

セキュリティ管理処理部１０は、図１に示すように機能ブロックとして、ＡＣＣ判定部２１，距離判定部２２，接近物解析部２３，異常判定部２４，セキュリティモード変更部２５，置き忘れ判定部２６，手動変更判定部２０およびセキュリティモード変更判定部２７を備えている。

【００７４】

手動変更判定部２０は、通信部４を介してセキュリティコントローラ３から送信された指示に応じて警戒モードの設定または解除を決定するものである。

【００７５】

手動変更判定部２０は、決定した結果をセキュリティモード変更部２５に送信する。

【００７６】

ＡＣＣ判定部２１は、ＡＣＣ検出部６によって検出されたＡＣＣ電源のＯＮ，ＯＦＦの情報を判定するものである。ＡＣＣ判定部２１は、この判定結果をセキュリティモード変更判定部２７に送信する。

【００７７】

距離判定部２２は、通信部４を介して受信したセキュリティコントローラ３ａ～３ｃから受信した電波の強度に基づき、セキュリティコントローラ３ａ～３ｃのそれぞれの位置を確認するものである。この距離判定部２２は、通信部４に対し、応答電波の送信要求を行う制御コマンド（電波要求コマンド）を、各セキュリティコントローラ３ａ～３ｃに送

信するように指示する。なお、この電波要求コマンドとは、セキュリティコントローラ３に対して、電波をセキュリティ装置２に送信するように指示するコマンドであり、例えばＰＩＮＧコマンドなどによって実現できる。

【００７８】

すなわち、距離判定部２２からの指示に応じて、通信部４がシステムコントローラ３に対して電波を送信するように電波要求コマンドを送信する。一方、セキュリティコントローラ３は、このコマンドに応じて、電波を通信部４に向けて送信する。

【００７９】

通信部４は受信したこの電波を距離判定部１２に渡す。そして、距離判定部２２は、通信部４を介して受信したセキュリティコントローラ３の電波強度から、セキュリティ装置２から各セキュリティコントローラ３までの距離を検出する。すなわち、より正確には距離判定部２２は、これらセキュリティコントローラ３ａ～３ｃがセキュリティ管理領域５０内にあるか否か、セキュリティコントローラ３ａ～３ｃのいずれかが一定の場所に留まっているかなどを解析する。この解析は所定時間間隔で行われ、距離判定部２２は、解析した結果を記憶部１１にセキュリティコントローラ監視テーブルとして記録する。

【００８０】

接近物解析部２３は、接近物検出部７の検出結果に基づき、セキュリティ管理対象である車に接近する人がいるか否かを判定するものである。セキュリティモード変更判定部２７からの指示に応じて、この接近物解析部２３は、接近物検出部７にセキュリティ管理対象の車に接近する人等を検出するように指示を出す。なお、接近物検出部７と接近物解析部２３とによって、人行動監視手段は実現される。

【００８１】

異常判定部２４は、異常検出部８からの検出結果に基づき、セキュリティ管理対象の車に異常状態が生じているか否かを判定するものである。異常判定部２４は、判定した結果、セキュリティ管理対象である車に異常が生じている場合は、威嚇部５に警戒音を発生させるように指示を出す。

【００８２】

セキュリティモード変更判定部２７は、セキュリティ管理対象の車に対するセキュリティモードの変更の有無を判定するものである。セキュリティモード変更判定部２７は、このセキュリティモードの変更の有無を、距離判定部２２および接近物解析部２３の判定結果に基づき、モード設定情報３１を参照して決定する。このモード設定情報３１の詳細は後述する。

【００８３】

また、セキュリティモードとは、警戒モード，非警戒モード，警戒待ち（警戒準備）モードという３つのモードであって、これらもモードが、本実施の形態に係るセキュリティ装置２において定義されている。

【００８４】

上記警戒モードとは、セキュリティ管理対象の車に正規のユーザ以外がセキュリティ管理領域５０内に侵入した場合、威嚇部５が警戒音等を発生して威嚇するように設定されたモードである。また、非警戒モードとは、正規ユーザのみならず、いかなる人がセキュリティ管理領域５０内に侵入しても威嚇等行われることがない、上記警戒モードの設定が解除されたモードである。

【００８５】

警戒待ち（警戒準備）モードとは、警戒モードと非警戒モードとのモードの移行期間のモードである。このモードにおいて、セキュリティ装置２は、距離判定部２２，ＡＣＣ判定部２１，接近物解析部２３から得られる情報等に基づいて、警戒モードから非警戒モードに、あるいは非警戒モードから警戒モードに移行するかを決定する。

【００８６】

セキュリティモード変更判定部２７は、決定したモードへの変更指示を置き忘れ判定部２６に送信する。

【００８７】
置き忘れ判定部２６は、セキュリティ管理対象である車にセキュリティコントローラ３ａ～３ｃのいずれかが置き忘れていないかを決定するものである。なお、置き忘れ判定の詳細な説明は後述する。
【００８８】
置き忘れ判定部２６は、車内にセキュリティコントローラ３ａ～３ｃのいずれかが置き忘れられているか否かの判定と、セキュリティモード変更判定部２７から送信された上記モードの設定指示とに基づき、セキュリティモード変更部２５にモードの切替えを指示する。
【００８９】
また、置き忘れ判定部２６は、車内にセキュリティコントローラ３ａ～３ｃのいずれかの置き忘れがあると判定した場合、置き忘れがある旨の通知を、通信部４を介して全てのセキュリティコントローラ３に対して通知する。
【００９０】
セキュリティモード変更部２５は、置き忘れ判定部２６からの指示またはユーザのセキュリティコントローラ３による指示に応じて、セキュリティ装置２の上記モードを切替えるものである。具体的には、セキュリティモード変更部２５は、威嚇部５を警戒設定にしたり、威嚇部５を非警戒モードにしたりする。なお、セキュリティモード変更部２５はい各部５に指示を出す最終的に設定されるモードをモード設定情報３１として記憶部１１に記憶する。
【００９１】
なお、威嚇部５は、警戒モードの設定がなされている場合のみ、異常判定部２４から異常の通知を受けて威嚇を行う。したがって、警戒設定が解除されている際に、異常判定部２４から異常の通知を受信したとしても威嚇部５は威嚇を行うことはない。
【００９２】
次に、記憶装置１１に記録されているセキュリティコントローラ監視テーブル３０およびモード設定情報３１について説明する。
【００９３】
セキュリティコントローラ監視テーブル３０は、図５に示すようにセキュリティコントローラ３ａ～３ｃそれぞれの電波強度を時系列に記録したテーブルである。このテーブルは、距離判定部２２が通信部４を介して各セキュリティコントローラ３ａ～３ｃから受信した電波強度を一定の間隔で記録する。図５は、本実施の形態に係るセキュリティ監視テーブル３０の一例を示す図である。
【００９４】
ところで、本実施の形態に係るセキュリティ装置２では、あらかじめ、セキュリティ管理領域５０とそれ以外の領域との境界位置からセキュリティ装置２までの間における、セキュリティコントローラ３の電波強度（基準電波強度と称する）について記憶されている。従って、セキュリティ装置２は、このセキュリティコントローラ監視テーブル３０を参照することで、どのセキュリティコントローラ３がセキュリティ管理領域５０内にあるか否かについて調べることができる。また、現在と過去における各セキュリティコントローラ３の電波強度を記録しているため、セキュリティ装置２は、現在と過去の両者の電波強度を調べることで、セキュリティコントローラ３がセキュリティ管理対象の車から遠ざかっているのか、近づいているのかについて知ることもできる。
【００９５】
さらに予め、セキュリティ管理対象の車の内と外（ユーザが車の乗降口に降り立った位置）とにおける電波強度について記憶されている。このことによって、セキュリティ管理領域５０内にある場合であっても車の内にセキュリティコントローラ３があるのか、車の外にあるのか判定することができる。
【００９６】
なお、セキュリティコントローラ３ａ～３ｃそれぞれの特定は、予め各コントローラ３

のＩＤがセキュリティ装置２に記録されており、このＩＤによって受信した電波強度がどのセキュリティコントローラ３から送信されたものであるかを決定することができる。

【００９７】

本実施の形態に係るセキュリティコントローラ管理テーブル３０は、現在の電波強度とその所定時間前の電波強度の２つを記録しているが、この２つに限定されるものではなく、２より多い時間間隔で測定した電波強度を記録してもよい。この場合は、より細かい電波強度の経時的な変化をしることができるためセキュリティコントローラの位置や移動の有無の検知精度が上がる。

【００９８】

また、セキュリティ装置２において距離判定部２２は、過去測定された電波強度のうち直前の電波強度のみを記録するように設定し、距離判定部２２が通信部４を介して取得した現在の各セキュリティコントローラ３の電波強度と、この管理テーブル３０に記録された電波強度とを比較する構成であってもよい。この場合は、過去に測定された電波強度のうち、直近の電波強度のみを記録しておくだけでよいため、使用する記録領域のメモリを最低限に抑える必要ができる。

【００９９】

また、本実施の形態に係るセキュリティ装置２では各セキュリティコントローラ３のＩＤを予め記憶することで、セキュリティ装置２は、各セキュリティコントローラ３を特定する構成であった。しかし、予め各セキュリティコントローラ３に使用される電波の周波数を異ならせ、各セキュリティコントローラ３を特定する構成であってもよい。さらには、各セキュリティコントローラ３からセキュリティ装置２に対して送信する電波の送信タイミングを所定の時間だけずらすように設定することで、各セキュリティコントローラ３を特定する構成であってもよい。

【０１００】

モード設定情報３１は、現在セキュリティ装置２において設定されているセキュリティモードを示す情報である。すなわち、このモード設定情報３１は、セキュリティモード変更部２５が威嚇部５に対してモードの設定を指示するとともに、この指示したモードの設定について記録する。

【０１０１】

（セキュリティコントローラの構成）

次に、図６を参照してセキュリティコントローラ３の構成について説明する。図６は、セキュリティコントローラ３の概略構成の一例を示すブロック図である。

【０１０２】

セキュリティコントローラ３は、コマンド入力部４０，通信部４１，通知部４２，コントローラ制御部４３，および識別情報記憶部４４を備えている。

【０１０３】

コマンド入力部４０は、ユーザが入力操作等を行うためのものである。ユーザによって入力された情報はコントローラ制御部４３に送信される。

【０１０４】

通信部４１は、他のセキュリティコントローラ３や、セキュリティ装置２との通信を行うものである。通信部４１は、他のセキュリティコントローラ３またはセキュリティ装置２に対して制御コマンド等を送信する。また、セキュリティコントローラ３は、セキュリティ装置２からＰＩＮＧコマンドを受信するとこのコマンドをコントローラ制御部４３に送信する。そしてコントローラ制御部４３は、コマンドを解読し通信部４１に当該セキュリティ装置２に電波を送信するように指示を出す。この指示に応じて通信部４１は電波をセキュリティ装置２に対して送信する。

【０１０５】

通知部４２は、セキュリティ装置４２または他のセキュリティコントローラ３から送信されたコマンドの内容をユーザに対して通知するものである。通知部４２は、例えば液晶ディスプレイなどの表示装置や、音声マイク等によって実現できる。

【０１０６】
コントローラ制御部４３は、上記したコマンド入力部４０，通信部４１，および通知部４２の各部材の各種制御を行うものである。
【０１０７】
識別情報記録部４４は、通信先である他のセキュリティコントローラ３およびセキュリティ装置２とを特定するための情報であって、自装置，自装置以外のセキュリティコントローラ３，およびセキュリティ装置２のＩＤ情報である。
【０１０８】
なお、上記したセキュリティコントローラ３の機能ブロックは、上記コマンド入力部４０，通信部４１，および通知部４２の各部材がバスを介してＣＰＵ，ＲＯＭ，およびＲＡＭと接続されており、ＣＰＵがＲＯＭに記録されたプログラムをＲＡＭに読み出し実行することで実現できるし、各機能を実現するＩＣを備えることによっても実現できる。
【０１０９】
（警戒設定待ち処理）
次に、本実施の形態に係るセキュリティ装置２における非警戒の状態（非警戒モード）から警戒状態（警戒モード）に移行する処理、すなわち警戒待ち処理の一例について説明する。なお、図７は、本実施の形態に係るセキュリティ装置２における警戒待ち処理の一例を示すフローチャートである。
【０１１０】
まず、セキュリティ装置２は車のＡＣＣ電源が「オン」から「オフ」に切り換わったか否かを判定する（ステップＳ１０、これ以降においてはＳ１０のように称する）。すなわち、セキュリティ装置２では、ＡＣＣ判定部２１が、ＡＣＣの電源が「オン」から「オフ」に切り換わるか否かを監視しており、ＡＣＣの電源が「オフ」へと切り換わらない限り（Ｓ１０において「Ｎｏ」の場合）、非警戒モードのままである。
【０１１１】
そして、ステップＳ１０において「Ｙｅｓ」の場合、すなわち、ユーザが車のエンジンのキーを回し電源を切ってＡＣＣ電源が「オン」から「オフ」に切り換わると、セキュリティ装置２は、ＡＣＣの電源が「オフ」になってから１０分以上経過したか否かを判定する（Ｓ１１）。
【０１１２】
つまり、本実施の形態に係るセキュリティ装置２では、１０分以上経過する間に、警戒モードに移行するための条件が満たされない場合は、非警戒モードのままとする設定となっている。
【０１１３】
ここまでの処理において１０分以上経過していない場合（ステップＳ１１において「Ｎｏ」）、次にセキュリティ装置２は、セキュリティコントローラ３ａ～３ｃが、セキュリティ管理領域５０外を出たか否かを判定する（Ｓ１２）。すなわち、セキュリティ装置２において、距離判定部２２が、各セキュリティコントローラ３ａ～３ｃから受信した電波強度をセキュリティコントローラ監視テーブル３０に記録している。そして、予め記憶されている基準電波強度と、現在受信しているセキュリティコントローラ３ａ～３ｃの電波強度とを比較し、現在受信している上記電波強度が、基準電波強度よりも大きいか小さいかを調べることによってこの判定ができる。
【０１１４】
つまり、セキュリティコントローラ監視テーブル３０に記録されているセキュリティコントローラ３の電波強度の履歴と、現在の受信しているセキュリティコントローラ３の電波強度それぞれとを比較し、セキュリティコントローラ３のそれぞれの電波強度が基準電波強度よりも大きい状態から小さい状態に変化した場合、このセキュリティコントローラ３はセキュリティ管理領域５０外に出たと判定できる。
【０１１５】
ステップＳ１０～ステップＳ１２までの処理経過時間内に、セキュリティコントローラ

３がセキュリティ管理領域５０外に出ていない場合（Ｓ１２において「Ｎｏ」）、セキュリティ装置２はセキュリティコントローラ３ａ～３ｃのいずれかから警戒モードへの変更を指示するコマンドが送信されたか否かを判定する（Ｓ１３）。

【０１１６】

一方、セキュリティコントローラ３がセキュリティ管理領域５０外に出ている場合（Ｓ１２において「Ｙｅｓ」）は、車内に置き忘れたセキュリティコントローラ３があるか否かを判例する（Ｓ１７）。

【０１１７】

なお通常、ステップＳ１０～ステップＳ１２までの処理経過時間は非常に短時間である。このため、最初にセキュリティ装置２がステップＳ１２の判定を行う場合はＡＣＣの電源が「オフ」になったばかりで、セキュリティコントローラ３ａ～３ｃのいずれもセキュリティ管理領域５０内にある可能性が高い。したがって、最初にセキュリティ装置２がステップＳ１２の判定を行う場合は、通常は次のステップＳ１３に進むこととなる。

【０１１８】

そこで、次に、セキュリティ装置２は、ステップＳ１３においてユーザの指示に応じて、セキュリティコントローラ３ａ～３ｃのいずれかから警戒モードに変更するよう指示するコマンドが送信されたか否かを判定する。

【０１１９】

そして、セキュリティ装置２がセキュリティコントローラ３ａ～３ｃのいずれかから警戒モードに変更するよう指示するコマンドを受信していないと判定した場合（ステップＳ１３において「Ｎｏ」）は、ステップＳ１１に戻る。また、ステップ１３において「Ｙｅｓ」の場合は、置き忘れのセキュリティコントローラ３があるか否かを判定する（Ｓ１４）。

【０１２０】

すなわち、セキュリティ装置２では、ユーザから直接警戒モードへの変更指示が送信される、あるいはセキュリティコントローラ３がセキュリティ管理領域５０外にでるまで、ステップＳ１１～Ｓ１３を繰り返す。そして。このステップＳ１１～Ｓ１３の判定処理の間に、ＡＣＣの電源が「オフ」になってから１０分以上経過した場合は、警戒設定を行わない（Ｓ１１「Ｙｅｓ」）ように構成されている。

【０１２１】

次に、ステップＳ１３の判定において、セキュリティ装置２が、セキュリティコントローラ３ａ～３ｃのいずれかから警戒モードへの変更指示を示すコマンドを、受信した場合、セキュリティコントローラ３ａ～３ｃのうち車内に置き忘れられたものがあるか否かを判定する（Ｓ１４）。この判定において、セキュリティ装置２がセキュリティコントローラ３ａ～３ｃのうち車内に置き忘れられたものがあると判定した場合（Ｓ１４において「Ｙｅｓ」）、セキュリティコントローラ３の置き忘れをユーザに通知する（Ｓ１５）。一方、セキュリティ装置２が、置き忘れのセキュリティコントローラ３がないと判定した場合（Ｓ１４において「Ｎｏ」）は、警戒モードに設定を変更する（Ｓ１６）。

【０１２２】

また、ステップＳ１７において車内に置き忘れたセキュリティコントローラ３があるか否かを判定した結果（Ｓ１７）、上記置き忘れたセキュリティコントローラ３がある場合は、ステップＳ１５に進む。一方、車内に置き忘れたセキュリティコントローラ３がない場合はステップＳ１６に進む。これ以降の処理は上記にて説明したため省略する。

【０１２３】

なお、セキュリティ装置２におけるセキュリティコントローラ３の置き忘れの判定および、セキュリティコントローラ３の置き忘れがある場合のユーザへの通知方法の詳細は後述する。

【０１２４】

以上が本実施形態に係るセキュリティ装置２における処理フローの一例である。ここで、セキュリティコントローラ３についての置き忘れ判定がない構成の場合の警戒設定待ち

処理を比較例として図８を参照して説明する。図８は、本実施の形態に係るセキュリティ装置２の比較例における警戒待ち処理の一例を示すフローチャートである。

【０１２５】

比較例の処理ステップでは、ステップＳ１１０～ステップＳ１１３までの処理フローは、上記した処理フローのステップＳ１０～ステップＳ１３までの処理と同じであるため、説明は省略する。

【０１２６】

この比較例では、ステップ１１２において、セキュリティコントローラ３がセキュリティ管理領域５０外に出た場合、セキュリティ装置２は警戒モードへの設定変更を行う。あるいはステップＳ１１３において、セキュリティコントローラ３から警戒モードへの変更指示を示すコマンドが送信される場合、セキュリティ装置２は警戒モードへの設定変更を行う。したがって、これら２点が比較例では本実施の形態に係るセキュリティ装置２の処理フローとは異なることとなる。

【０１２７】

つまり、本実施形態に係るセキュリティ装置２では、警戒モードに設定変更する直前の処理において置き忘れたセキュリティコントローラ３の有無の判定を行い、セキュリティコントローラ３の置き忘れがある場合は、それを通知できる。

【０１２８】

したがって、車内にセキュリティコントローラ３が置き忘れられた場合、ユーザにこの置き忘れられたセキュリティコントローラ３があることをユーザに通知することができる。また、セキュリティ装置２は、上記通知を行った後に、セキュリティ管理対象の車５１を警戒状態に設定する構成である。

【０１２９】

つまり、セキュリティ装置２は、置き忘れられたセキュリティコントローラ３が車内にある場合、ユーザにセキュリティコントローラ３の置き忘れに対する注意を促した上で車を警戒モードの設定に切り替えることができる。

【０１３０】

また、置き忘れられたセキュリティコントローラ３が車内にあるため、セキュリティ装置２が、ユーザがまだ車内にいる状態ととらえ非警戒状態のままとすることを防ぐ構成でもある。したがって、セキュリティ装置２は、セキュリティコントローラ３ａ～３ｃいずれかを置き忘れた場合であっても、非警戒モードのままにして正規ユーザ以外の人の接近を許し被害に遭うことを防止することができる。

【０１３１】

一方、比較例では、セキュリティコントローラ３から警戒モードへの設定指示を示すコマンドを受信したり、セキュリティコントローラ３がセキュリティ管理領域５０外に移動したりすると警戒モードに設定される構成である。

【０１３２】

このため、この比較例は、本実施の形態に係るセキュリティ装置２と同様にセキュリティコントローラ３ａ～３ｃいずれかを置き忘れた場合であっても、非警戒モードのままにして正規ユーザ以外の人の接近を許し被害に遭うことを防止することができる。

【０１３３】

しかし、警戒モードに設定された後、セキュリティコントローラ３がセキュリティ装置２の近くに置き忘れられているため、ユーザ以外の人が車に接近するだけで警戒モードを解除してしまうということが、ユーザが知らない間に発生することとなる。

【０１３４】

（警戒処理および警戒解除処理）

次は逆に警戒モードに設定されている状態から、この警戒状態を解除するまでの警戒処理について図９を参照して説明する。図９は、本実施の形態に係るセキュリティ装置２における警戒処理および警戒処理解除の一例を示すフローチャートである。

【０１３５】

まず、前提としてセキュリティ管理対象である車において警戒モードが設定されている状況からこの処理の説明を行うものとする。

【０１３６】

セキュリティ装置２は、警戒モードに設定されている間、セキュリティコントローラ３ａ～３ｃのいずれかから警戒モードの解除指示を示すコマンドが送信されたか否かを判定する（Ｓ２０）。

【０１３７】

セキュリティ装置２は、セキュリティコントローラ３ａ～３ｃの何れからも警戒モードの解除指示を示すコマンドを受信していない場合（Ｓ２０においてＮｏ）、セキュリティ管理対象である車に異常が生じているか否かを判定する（Ｓ２１）。

【０１３８】

一方、セキュリティ装置２が、セキュリティコントローラ３ａ～３ｃの何れから警戒モードの解除指示を示すコマンドを受信した場合（Ｓ２０においてＹｅｓ）は、設定されている警戒モードを解除して非警戒モードとする。

【０１３９】

すなわち、通信部４を介してセキュリティコントローラ３から受信した警戒モードの解除指示を示すコマンドを、通信部４を介してセキュリティモード変更部２５が受信する。そしてセキュリティモード変更部２５は、この受信したコマンドに応じて威嚇部５に対して警戒モードの設定を解除するように指示を出すとともに、モード設定情報３１を警戒モードから非警戒モードに書き換える。

【０１４０】

つまり、本実施形態に係るセキュリティ装置２では、ユーザが、所持しているセキュリティコントローラ３から警戒モードの設定の解除指示を行う場合、警戒解除を即座に行える構成となっている。

【０１４１】

ステップＳ２１において、セキュリティ装置２が、セキュリティ管理対象の車に異常が生じていないと判定した場合（Ｓ２１において「Ｙｅｓ」）、人の接近の有無を判定する（Ｓ２２）。　一方、ステップＳ２１において、セキュリティ装置２がセキュリティ管理対象である車に異常が生じたと判定した場合、異常が発生したことをセキュリティコントローラ３ａ～３ｃに通知し（Ｓ２６）、威嚇を行う（Ｓ２７）。そして、セキュリティ装置２は、しばらく威嚇を行った後、再度に警戒状態に戻る。

【０１４２】

すなわち、異常検出部８を介して、異常判定部２４がセキュリティ管理対象の車に異常が生じていると判定した場合、異常の発生を、通信部４を介してセキュリティコントローラ３ａ～３ｃに通知するとともに、威嚇部５にも威嚇動作を行うように指示を出す。威嚇部５は、セキュリティモード変更部２５によって警戒モードに設定されているため、異常判定部２４から威嚇動作の指示を受けると、警報音を発生させたり、発光させたりする。

【０１４３】

ステップＳ２２において、セキュリティ装置２が人の接近を検知した場合（Ｓ２２において「Ｙｅｓ」）は、セキュリティ装置２の近くにセキュリティコントローラ３ａ～３ｃの何れかがあるか否かを判定する（Ｓ２３）。

【０１４４】

一方、セキュリティ装置２が、人の接近を検知しない場合（Ｓ２２において「Ｎｏ」）、ステップＳ２０に戻る。すなわち、Ｓ２０～Ｓ２２の間の検知を繰り返すこととなる。

【０１４５】

次に、ステップＳ２３の判定において、セキュリティ装置２が自装置の近くにセキュリティコントローラ３ａ～３ｃの何れかがあると判定した場合（Ｓ２３）、すなわちセキュリティ管理領域５０内にセキュリティコントローラ３ａ～３ｃの何れかがあると判定した場合、セキュリティコントローラ３ａ～３ｃの何れかのうち置き忘れられたものがあるか否かを判定する（Ｓ２４）。

【０１４６】
一方、近くにセキュリティコントローラ３ａ～３ｃの何れかが無いと判定した場合は、ステップＳ２０に戻る。
【０１４７】
すなわち、セキュリティ装置２は、人の接近を検知し（Ｓ２２において「Ｙｅｓ」）、かつセキュリティ管理領域５０内にセキュリティコントローラ３ａ～３ｃの何れかが存在する（Ｓ２３において「Ｎｏ」）まで、セキュリティコントローラ３からの警戒モードの設定解除指示があるか否か（Ｓ２０），セキュリティ管理対象の車に異常が生じたか否か（Ｓ２１）を繰り返し判定する構成である。
【０１４８】
ステップＳ２３において、セキュリティ装置２が自装置の近く、すなわちセキュリティ管理領域５０内にセキュリティコントローラ３ａ～３ｃの何れかが存在すると判定した場合（Ｓ２３において「Ｙｅｓ」）、セキュリティコントローラ３ａ～３ｃの何れかのうち置き忘れられたものがあるか否かを判定する（Ｓ２４）。
【０１４９】
置き忘れられたセキュリティコントローラ３があると判定した場合（Ｓ２４において「Ｙｅｓ」）は、再度ステップ２０からの処理を繰り返す。
【０１５０】
一方、置き忘れられたセキュリティコントローラ３がないと判定した場合（Ｓ２４において「Ｎｏ」）、警戒解除を行う（Ｓ２５）。
【０１５１】
すなわち、置き忘れられたセキュリティコントローラ３があると判定した場合、置き忘れられたセキュリティコントローラ３と正規のユーザ以外の接近という組み合わせがあるため、セキュリティ装置２は警戒モードを解除しない。このため、セキュリティ装置２では、正規ユーザは、セキュリティコントローラ３からセキュリティ装置２に対して警戒モードの設定解除を指示するコマンドを送信することで警戒モードを解除する必要がある。
【０１５２】
このようにして、本実施形態に係るセキュリティ装置２は、セキュリティコントローラ３ａ～３ｃの何れかが置き忘れられた場合であっても、この置き忘れられたセキュリティコントローラ３ａ～３ｃのいずれかと、人との接近という組み合わせで警戒モードの設定を誤って解除することを防ぐことができる。
【０１５３】
以上が本実施形態に係るセキュリティ装置２における警戒処理および警戒解除処理の一例である。ここで、セキュリティコントローラ３の置き忘れ判定がない構成の場合の処理フローを比較例として図１０を参照して説明する。図１０は、本実施の形態に係るセキュリティ装置２の比較例における警戒処理および警戒解除処理の一例を示すフローチャートである。
【０１５４】
比較例の処理ステップでは、ステップＳ１２０～ステップＳ１２３，ステップＳ１２５～ステップＳ１２６までの処理フローは、上記した処理フローのステップＳ２０～ステップＳ２３，ステップＳ２５～ステップＳ２６までの処理と同じであるため、説明は省略する。
【０１５５】
この比較例では、ステップ１２３において、セキュリティ装置２が、セキュリティ管理領域５０内にセキュリティコントローラ３ａ～３ｃのいずれかが存在する場合、警戒解除を行う（Ｓ１２４）点が本実施の形態に係るセキュリティ装置２の処理フローとは異なることとなる。
【０１５６】
したがって、この比較例では、車内に置き忘れられたセキュリティコントローラ３がある場合、正規ユーザ以外がセキュリティ管理対象の車に接近したときでも、警戒モードの

設定を誤って解除することとなる。

【０１５７】

このため、本実施の形態に係るセキュリティ装置２では、置き忘れられたセキュリティコントローラ３と正規ユーザ以外の人の接近との組み合わせの場合は、警戒モードの設定を解除しない構成であるため、比較例の構成と比べてより好ましい構成であると言える。

【０１５８】

（置き忘れ判定処理）

次に置き忘れ判定処理について詳細に説明する。

【０１５９】

本実施の形態に係るセキュリティ装置２では、警戒モードへの設定条件が揃った場合、もしくはセキュリティコントローラ３ａ～３ｃの何れかから警戒モードへの設定指示のコマンドを受信した場合、セキュリティ管理領域５０内にあるセキュリティコントローラ３に対して警戒モードへの設定変更する旨の通知を行う。

【０１６０】

なお、この通知は、セキュリティコントローラ３の通知部４２が通知内容を表示することによって行われてもよいし、通知部４２が音声によって通知内容をユーザに通知する構成であってもよい。また、セキュリティコントローラ３の通知部４２がバイブレーション機能を有しており、振動によって通知する構成であってもよい。さらには表示と音声と振動とのうちのいずれかの組み合わせによってユーザに通知するものであってもよい。

【０１６１】

このように通知することによって正規のユーザが携帯するセキュリティコントローラ３であれば、この通知に対する応答が返されることとなる。しかし、置き忘れられたセキュリティコントローラ３の場合は、この通知に対する応答がないこととなる。

【０１６２】

したがって、セキュリティ装置２は、この通知に対して反応の無いセキュリティコントローラ３を置き忘れられたものと判定する。

【０１６３】

より具体的に言えば、まずセキュリティモード変更判定部２７が、ＡＣＣ判定部２１および距離判定部２２からの情報を受信すると、警戒モードへの設定変更の判定を行い、設定を変更する場合には警戒モードとなるように置き忘れ判定部２６に指示を出す。

【０１６４】

すなわち、セキュリティモード変更判定部２７は、ＡＣＣ判定部２１からＡＣＣの電源が「オン」から「オフ」に切り換わったという情報と、距離判定部２２から、セキュリティコントローラ３ａ～３ｃの何れかがセキュリティ管理領域５０内からセキュリティ管理領域５０外に出たという情報とを受信した場合、警戒モードへの設定変更指示の情報を置き忘れ判定部２６に送信する。

【０１６５】

置き忘れ判定部２６は、セキュリティモード変更判定部２７からの上記情報を受信すると、セキュリティコントローラ監視テーブル３０を参照して、セキュリティ管理領域５０内にあるセキュリティコントローラ３を特定する。

【０１６６】

そして、置き忘れ判定部２６は、特定した上記セキュリティコントローラ３に対して通信部４を介して応答を要求するコマンド（応答要求コマンド）を送信する。置き忘れ判定部２６は、所定期間(例えば５分間)待って、通知先のセキュリティコントローラ３から応答コマンドに対する返答が来ない場合は、このセキュリティコントローラ３は置き忘れられたものであると判定する。

【０１６７】

また、この応答要求コマンドに対する返答として、警戒モードへの設定変更を要求するコマンドをセキュリティコントローラ３ａ～３ｃの何れかから受信した時点で、セキュリティ管理領域５０内にあるセキュリティコントローラ３を置き忘れとする構成であっても

よい。

【０１６８】

また、上記応答要求コマンドに対して最初に応答してきたセキュリティコントローラ３以外のセキュリティ管理領域５０内にあるセキュリティコントローラ３を置き忘れられたものとして判定する構成でもよい。この場合は、セキュリティ装置２は、セキュリティ領域内にあるセキュリティコントローラ３のうち唯１つに対してオートセキュリティ機能可能とすることで、確実にユーザが携帯しているセキュリティコントローラ３のみをオートセキュリティ機能に対して有効とすることができる。

【０１６９】

従って、この場合は置き忘れら得たセキュリティリモコンを含むセキュリティ管理領域５０内にあるセキュリティコントローラ３において、特定のセキュリティコントローラ３以外はオートセキュリティ機能を有効としないことで誤って警戒モードが解除される可能性を低減させることができる。

【０１７０】

このように、本実施の形態に係るセキュリティ装置２は上記したように、セキュリティ管理領域５０内にあるセキュリティコントローラ３に対して応答要求コマンドを送信する、そして、この応答要求コマンドに対する返答の状態によって、セキュリティ管理領域５０内にあるセキュリティコントローラ３に対して置き忘れか否かを判定する構成である。

【０１７１】

このため、例えば、正規ユーザが車の洗車などをおこなっており、セキュリティ管理領域５０内に存在する場合であっても、応答要求コマンドに対する返答として警戒モードの設定を行わないように促す内容を通知することで、誤って警戒モードに設定されることを防ぐことができる。

【０１７２】

さらに、本実施形態に係るセキュリティ装置２において、上記セキュリティコントローラ３の置き忘れ判定を以下のように行う構成とすることもできる。

【０１７３】

すなわち、セキュリティコントローラ３ａ～３ｃの何れかから警戒モードへの設定指示を示すコマンドを受信した場合、所定期間（例えば５分間）経過した後、セキュリティ管理領域５０内にセキュリティコントローラ３ａ～３ｃの何れかがある場合は、このセキュリティ管理領域５０内のセキュリティコントローラ３を置き忘れられたものと判定する構成であってもよい。

【０１７４】

あるいは、上記したようにセキュリティモード変更判定部２７が警戒モードへの設定変更の条件を満たすと判定した場合、所定期間（例えば５分間）経過した後、セキュリティ管理領域５０内にセキュリティコントローラ３ａ～３ｃの何れかがある場合は、このセキュリティ管理領域５０内のセキュリティコントローラ３を置き忘れられたものと判定する構成であってもよい。

【０１７５】

また、上記所定期間を例えば３０分間というように、ある程度長い期間に設定し、この間においてセキュリティ管理領域５０内に留まっているセキュリティコントローラ３があれば、これを置き忘れられたものとみなしてもよい。この場合は、セキュリティ管理領域５０内にあるセキュリティコントローラ３の動向をより精度良く観察した上で置き忘れられたものか否かを判定できる。

【０１７６】

つまり、セキュリティモード変更判定部２７が、通信部４を介してセキュリティコントローラ３ａ～３ｃのいずれかから警戒モードへの設定変更指示を受信する、あるいは、ＡＣＣ判定部２１および距離判定部２２から送信された情報に基づき、警戒モードに設定を変更すると判定すると、置き忘れ判定部２６に警戒モードへの設定変更指示を送信する。

【０１７７】

そして、置き忘れ判定部２６は、セキュリティモード変更判定部２７からの指示を受信すると、所定時間経過後にセキュリティコントロール監視テーブル３０を参照して、セキュリティ管理領域５０内にあるセキュリティコントローラ３を置き忘れであると特定する。

【０１７８】

また、セキュリティモード変更判定部２７が警戒モードへの設定変更の条件を満たすと判定した場合、セキュリティ管理領域５０内にあるセキュリティコントローラ３を置き忘れられたものと判定する構成であってもよい。

【０１７９】

これらの場合は、置き忘れ判定部２６がセキュリティコントローラ監視テーブル３０の情報のみを参照して置き忘れを判定できる。このため、上記したセキュリティ管理領域５０内にあるセキュリティコントローラ３に応答を要求する構成よりもより簡単な構成でセキュリティコントローラ３の置き忘れに関する判定ができる。

【０１８０】

しかし、複数ユーザのうち一部のユーザが車内に残ってセキュリティコントローラ３を保持している場合も、このセキュリティコントローラ３を置き忘れとするため、置き忘れか否かの判定精度の点では、本実施形態に係るセキュリティ装置２の構成の方が好ましい。

【０１８１】

また、上記置き忘れ判定部３の置き忘れ判定の精度を高めるために、セキュリティコントローラ３とセキュリティ装置２は以下の構成をさらに備えていてもよい。

【０１８２】

すなわち、セキュリティコントローラ３は、例えば加速度センサまたは振動センサ（不図示）をさらに備え、ユーザの携帯によってセキュリティコントローラ３に生じる振動等の動きをセキュリティ装置２に伝えることができる。

【０１８３】

一方、セキュリティ装置２は、上記セキュリティコントローラ３から送信される振動等の動きの情報を検出する振動検出部（不図示）と、この検出結果からセキュリティコントローラ３に動きがあるか否かを判定する振動判定部（不図示）とをさらに備えた構成としてもよい。

【０１８４】

この場合は、セキュリティ装置２は、ユーザによって携帯されることによってセキュリティコントローラ３に生じる振動を検知することができる。したがって、置き忘れ判定部２６は、セキュリティコントローラ３がユーザによって所持されている状態であるのか否かという情報を、さらに上記した置き忘れ判定処理に加えることができることとなる。このため、セキュリティ装置２は、セキュリティ管理領域５０内にあるセキュリティコントローラ３が置き忘れられたものであるか否かの判定精度を高めることができる。

【０１８５】

また、セキュリティ装置２は、車内の人の動きを検出する、上記接近物検出部７と同様のドップラセンサ（不図示）と、セキュリティ管理処理部１０にこのドップラセンサからの情報を解析するドップラセンサ解析部（不図示）とをさらに備えた構成としてもよい。

【０１８６】

あるいは、シートにかかる人の重さを検出するために、車内のシート下に、所定の圧力以上を検出する圧力センサ（不図示）と、セキュリティ管理処理部１０に、この圧力センサからの情報を解析する圧力センサ解析部（不図示）とをさらに備えた構成であってもよい。そして、これらドップラセンサおよび／または圧力センサによって検知した情報に基づき、ドップラセンサ解析部および／または圧力センサ解析部が車内にユーザがいるか否かを判定する。そして、置き忘れ判定部２６は、これらドップラセンサ解析部および／または圧力センサ解析部による判定結果を、上記した置き忘れ判定処理を行う情報としてさらに用いる構成としてもよい。この場合は、車内におけるユーザの有無に関する情報をさ

らに置き忘れ判定処理に加えることとなる。

【０１８７】

このため、置き忘れ判定部２６は、セキュリティ管理領域５０内にあるセキュリティコントローラ３が置き忘れられたものであるのあるのか否かの判定精度を高めることができる。

【０１８８】

また、本実施形態に係るセキュリティ装置２は、上記したようにセキュリティ管理領域５０内にあるセキュリティコントローラ３に対する監視によって置き忘れを判定するだけではなく、セキュリティコントローラ３の置き忘れに気づいたユーザからの通知に対しても対処できる構成である。

【０１８９】

すなわち、セキュリティ装置２は、セキュリティ管理領域５０外のセキュリティコントローラ３ａ～３ｃのいずれから、車内にセキュリティコントローラ３ａ～３ｃのいずれかを置き忘れていることを通知する情報を受信した場合、この情報において指定されているセキュリティ管理領域５０内のセキュリティコントローラ３を置き忘れられたものとする。

【０１９０】

なお、セキュリティ管理領域５０外からなされるこの通知には、置き忘れたセキュリティコントローラ３のＩＤ等識別情報が含まれている。このため、セキュリティ装置２は、セキュリティ管理領域５０内にあるセキュリティコントローラ３のうちどれが置き忘れたものであるのか特定することができる。

【０１９１】

また、セキュリティ装置３ａ～３ｃのいずれかがセキュリティ管理領域５０内にある場合であっても、警戒設定を指示する要求を予め設定されている場合は、セキュリティ装置２は警戒モードへの設定変更の条件が揃った場合は、セキュリティ管理領域５０内にあるセキュリティリモコン３を置き忘れられたものとみなす構成であってもよい。

【０１９２】

（置き忘れ判定後の通知）

上記にて、「警戒処理および警戒解除処理」に説明したように、セキュリティ装置２が置き忘れられたセキュリティコントローラ３が車内にあると判定した場合、セキュリティ装置２はユーザに置き忘れられたセキュリティコントローラ３がある旨を通知するように構成されている。以下、この通知を行う処理について説明する。

【０１９３】

すなわち、セキュリティ装置２は、管理対象である車５１を警戒モードに設定する際に、置き忘れられたセキュリティコントローラ３があると判定すると、セキュリティコントローラ３ａ～３ｃに対して、セキュリティ管理領域５０内にセキュリティコントローラ３ａ～３ｃのいずれかが置き忘れられていることを通知する。

【０１９４】

そして、さらに通知したセキュリティコントローラ３以外のセキュリティコントローラ３の状態を表示させるように、セキュリティコントローラ３に情報を送信することが好ましい。これは、通知されたもの以外のセキュリティコントローラ３がセキュリティ管理領域５０内にあるか否かという情報を表示させることで、どのセキュリティコントローラ３が置き忘れられているものであり、どのセキュリティコントローラ３がユーザに携帯されたままセキュリティ管理領域５０内にあるのかを示すことができる。

【０１９５】

ところで、本実施の形態に係るセキュリティ装置２では、上記した通知をセキュリティコントローラ３ａ～３ｃに行った後、置き忘れ判定部２６は、警戒モードへの変更指示を示す情報をセキュリティモード変更部２５に送信するとともに、置き忘れられたセキュリティコントローラ３として特定したセキュリティコントローラ３の情報（不図示）を記憶部１１に記憶しておく。

【０１９６】
そして、セキュリティモード変更部２５は、置き忘れ判定部２６から受信した情報に基づき、警戒モードに設定するように威嚇部５に指示を出す。
【０１９７】
このようにして、セキュリティ装置２は、置き忘れられたセキュリティコントローラ３の有無を判定した後に、管理対象である車５１を警戒モードに設定するのである。
【０１９８】
また、管理対象である車５１が警戒モードに設定された後、セキュリティコントローラ３を携帯したユーザが管理対象の車５１に戻ってきた場合、セキュリティ装置２は、ユーザが携帯しているセキュリティコントローラ３によって警戒モードの解除を行うようにする。すなわち、セキュリティ装置２は、オートセキュリティ機能を停止し、ユーザが手動で警戒モードの設定を解除するまでは警戒モードの設定を解除しない構成である。
【０１９９】
また、セキュリティ装置２は、上記のようにオートセキュリティ機能を停止するのではなく、置き忘れられたセキュリティコントローラ３があると判定した場合、この置き忘れられたセキュリティコントローラ３に対して、電源を切るように指示する構成とすることで、誤って警戒モードの設定を解除することを防ぐこともできる。
【０２００】
このように本実施の形態に係るセキュリティ装置２では、警戒モードに設定する際に置き忘れ判定部２６が、セキュリティ管理領域５０内に置き忘れられたセキュリティコントローラ３があるか否かを判定することができる構成である。そして、置き忘れられたセキュリティコントローラ３がある場合、この置忘れられたセキュリティコントローラ３が存在することを示す情報をセキュリティコントローラ３ａ～３ｃに通知する構成である。そして、セキュリティ装置２は、この通知を行った後に警戒モードに設定を切り替えるように構成されている。
【０２０１】
すなわち、セキュリティ装置２は、置き忘れられたセキュリティコントローラ３が、セキュリティ管理領域５０内にあると判断した場合、このセキュリティコントローラ３の存在をユーザに認識させることができる。そして、ユーザに置き忘れられたセキュリティコントローラ３の存在を認識させた上で、管理対象である車５１を警戒モードに切り替えるように構成されている。このようにセキュリティ装置２は、セキュリティ管理対象である車５１が非警戒モードのままの設定とならないように構成されている。
【０２０２】
したがって、置き忘れられたセキュリティコントローラ３がある場合であっても、セキュリティ管理対象である車５１が非警戒状態のままとならず正規ユーザ以外の人によって被られる被害を防ぐことができる。
【０２０３】
さらには、セキュリティ装置２は、置き忘れられたセキュリティコントローラ３がある場合、オートセキュリティ機能による警戒モード設定の解除を行わないように構成されている。このため、セキュリティコントローラ３を所持しない人がセキュリティ管理対象である車５１に接近した場合、セキュリティ装置２は、置き忘れられたセキュリティコントローラ３と、この接近してきた人との組み合わせによって、誤って警戒モードの設定を自動的に解除することを防ぐことができる。
【０２０４】
（セキュリティ管理領域５０内にあるセキュリティコントローラへの通知）
上記にて、置き忘れられたセキュリティコントローラ３がある場合、セキュリティ装置２は、他のセキュリティコントローラ３に「置き忘れられたセキュリティコントローラ３」の存在を通知する。そして、セキュリティ装置２は、置き忘れられたセキュリティコントローラ３があることをユーザに認識させるため通知する構成であった。
【０２０５】

次に、セキュリティコントローラ３ａ～３ｃをそれぞれ所持する各ユーザの行動に応じて、セキュリティ装置２がさらに適切な通知を行う構成について説明する。

【０２０６】

本実施形態に係るセキュリティ装置２は、上記したように複数のセキュリティコントローラ３ａ～３ｃが登録されている。このため、セキュリティコントローラ３ａ～３ｃのそれぞれの位置関係に応じて、警戒モードの設定がどのタイミングで行われたかをユーザが把握できる必要がある。

【０２０７】

ところで、セキュリティ装置２は、上記したようにセキュリティコントローラ３ａ～３ｃのいずれかがセキュリティ領域内からセキュリティ領域外に移動した場合、オートセキュリティ機能によってセキュリティ管理対象の車５１が警戒モードに設定される構成である。

【０２０８】

しかし、複数のユーザがそれぞれ車５１から降車して移動するタイミングが異なる場合がある。そこで、どのセキュリティコントローラ３がセキュリティ管理領域５０から出た時点で警戒モードに設定するのかを決定する必要がある。

【０２０９】

本実施の形態に係るセキュリティ装置２では、警戒モードへの設定変更指示を出す条件は、ＡＣＣ電源がＯＦＦになって所定時間内、すなわち１０分間内にセキュリティ管理領域５０外に出て行くセキュリティコントローラ３がある場合としていた。この条件をより正確に言えば、１０分間内にセキュリティコントローラ３ａ～３ｃのいずれか１つがセキュリティ管理領域５０外に出て行く場合に警戒モードへの設定変更指示を出す条件である。

【０２１０】

したがって、セキュリティコントローラ３ａ～３ｃそれぞれを携帯するユーザが一斉にセキュリティ管理対象である車５１から出て略同時にセキュリティ管理領域５０内に出れば問題がない。また、ばらばらのタイミングで各ユーザがセキュリティ管理領域５０外に出る場合でも、警戒設定を行うか否かを決定する期間、すなわちＡＣＣの電源が「オン」から「オフ」に変わってから１０分間であれば問題がない。

【０２１１】

つまり、最初にセキュリティ管理領域５０外に出たユーザのセキュリティコントローラ３によって、一旦警戒モードの設定が指示されるが、次のユーザがセキュリティ管理領域５０内にいるため、この次のユーザのセキュリティコントローラ３によって警戒モードの解除指示が出され、この次のユーザがセキュリティ管理領域５０外に出た時点で再度警戒モードの設定指示が行われることとなる。

【０２１２】

したがって、セキュリティ装置２は、結果として最後のユーザがセキュリティ管理領域５０外に出た時点で警戒モードの設定指示を行うことができる。

【０２１３】

しかし、ＡＣＣの電源が「オン」から「オフ」に変わってから１０分間経過する間に、セキュリティコントローラ３を有するすべてのユーザがセキュリティ管理領域５０外に出ていない場合は、非警戒状態のままとなる。

【０２１４】

そこで、本実施の携帯に係るセキュリティ装置２は、上記図７に示す「警戒設定待ち処理」で説明したように、セキュリティコントローラ３がセキュリティ管理領域５０外に出てから所定期間（５分間）待って、セキュリティコントローラ３ａ～３ｃのいずれかにおいて置き忘れられたものがあるか否かの判定を行い、置き忘れられたセキュリティコントローラ３が無い場合は、警戒モードに設定を変更指示する構成となっている。

【０２１５】

すなわち、セキュリティ装置２は、１０分の間でセキュリティ管理領域５０外にセキュ

リティコントローラ３を所持して出た複数のユーザのうち、最後にこのセキュリティ管理領域５０外を出たユーザの時間から５分間経過した後に、置き忘れられたセキュリティコントローラ３があるか否かを判定する。

【０２１６】

したがって、まだ他にもユーザがセキュリティ管理領域５０内にいる場合であっても、このユーザが所持するセキュリティコントローラ３は置き忘れられたものではないため、セキュリティ装置２は警戒モードの設定変更指示を行うことができる。ただし、セキュリティ装置２は、セキュリティコントローラ３の置き忘れ判定が行われた際に、少なくともセキュリティ管理領域５０内にいるセキュリティコントローラ３に対して警戒状態に設定される旨の通知を行う。これは、セキュリティ管理領域５０内にいるユーザが知らない間に、セキュリティ管理対象である車５１が警戒モードの設定変更され、意図せぬ威嚇等を受けることを防ぐためである。

【０２１７】

なお、この通知は、セキュリティ管理領域５０内にあるセキュリティコントローラ３に対する通知のみならず、全てのセキュリティコントローラ３に対して行われる設定であってもよい。この場合は、他のセキュリティコントローラ３に対しても行うことで、他のユーザは、セキュリティ管理対象である車５１が警戒状態に設定されたことを確認することができる。

【０２１８】

ところで、本実施の形態に係るセキュリティ装置２は、セキュリティ管理対象である車５１に置き忘れられたセキュリティコントローラ３があると判定した場合、この判定結果に基づく通知を他のセキュリティコントローラ３に行った上で、セキュリティ管理対象である車５１に対して警戒モードの設定を行う構成であった。しかし、セキュリティ装置２を、上記通知後、警戒モードの設定を行わない構成としてもよい。

【０２１９】

すなわち、セキュリティ装置２は、セキュリティコントローラ３ａ～３ｃに、セキュリティコントローラ３ａ～３ｃのいずれかがセキュリティ管理対象である車５１に置き忘れているということを通知した後、警戒モードに設定を変更しないように構成されていてもよい。ただし、セキュリティ装置２は、警戒モードに設定を変更しないということをさらに、セキュリティ装置３ａ～３ｃに通知する。

【０２２０】

このようにして、セキュリティ装置２は、セキュリティコントローラ３ａ～３ｃのいずれかがセキュリティ管理領域５０内に置き忘れられているという通知と、警戒モードに設定を変更しないという通知との２回の通知を行うことで、ユーザに対応を促すことができる。また、セキュリティコントローラ３を置き忘れたユーザが、セキュリティ管理対象である車５１に戻ってきた時にも警戒モードに設定されていないため予期せず威嚇されることがない。

【０２２１】

さらにまた、セキュリティ装置２は、セキュリティ管理領域５０内にセキュリティコントローラ３があると判定した場合、この判定結果に基づく通知を他のセキュリティコントローラ３に行った上で、警戒モードの設定を行わない構成としてもよい。

【０２２２】

すなわち、セキュリティ装置２は、セキュリティコントローラ３ａ～３ｃに、セキュリティコントローラ３ａ～３ｃのいずれかがセキュリティ管理領域５０にあるということを通知した後、警戒モードに設定を変更しないように構成されていてもよい。ただし、セキュリティ装置２は、警戒モードに設定を変更しないということをさらに、セキュリティ装置３ａ～３ｃに通知する。好ましくは、セキュリティ管理領域５０内にあるセキュリティコントローラ３の情報を示す通知も行う。この通知を行うことで、ユーザはセキュリティ管理領域５０内にあるセキュリティコントローラ３を確認することができ、この確認の上で、警戒モードに設定するあるいは設定しないという指示セキュリティ装置２に指示する

ことができる。

【０２２３】

このようにして、セキュリティ装置２は、セキュリティコントローラ３ａ～３ｃのいずれかがセキュリティ管理領域５０内にあるという通知と、警戒モードに設定を変更しないという通知との２回の通知を行うことで、ユーザに対応を促すことができる。また、セキュリティコントローラ３を置き忘れたユーザが、セキュリティ管理対象である車５１に戻ってきた時にも警戒モードに設定されていないため予期せず威嚇されることがない。また、セキュリティ管理領域５０内にいるユーザの知らない間に、セキュリティ管理対象の車５１が警戒モードに設定され、このユーザが予期せぬ威嚇を受けることを防ぐことができる。

【０２２４】

さらにまた、セキュリティ装置２は、セキュリティ管理領域５０内にセキュリティコントローラ３があると判定した場合、例えユーザから警戒モードへの変更指示が出された場合であっても警戒モードの設定を行わない構成としてもよい。

【０２２５】

ただし、セキュリティ装置２は、警戒モードに設定を変更しないということをさらに、セキュリティ装置３ａ～３ｃに通知する。そして、この通知に応じて再度ユーザが警戒モードへの設定変更を指示した場合は、警戒モードに設定を変更する。

【０２２６】

このように、セキュリティコントローラ３による警戒モードへの設定指示を行えないようにすることで、ユーザにセキュリティ管理領域５０内にセキュリティコントローラ３が存在することを知らせることができる。すなわち、通常行えるはずのセキュリティコントローラ３の操作とは異なる挙動をセキュリティ装置２が行うことで、ユーザにセキュリティ管理領域５０内にあるセキュリティコントローラ３の存在に気づかせることができるのである。　また、セキュリティ管理対象の車５１の複数ユーザの全てが同じ場所に居合わせている場合、ユーザは、セキュリティ管理領域５０内にあるセキュリティコントローラ３は複数ユーザのうちの何れかが置き忘れたセキュリティコントローラ３であることが分かる。

【０２２７】

さらにまた、他のセキュリティコントローラ３によって警戒モードに設定指示されている場合、設定解除処理の置き忘れられたセキュリティコントローラ３があるか否かの判定において、例えば３０分間以上の長時間セキュリティ管理領域５０内にあるセキュリティコントローラ３は全て置き忘れられたセキュリティコントローラ３とするように構成してもよい。

【０２２８】

すなわち、この場合、長時間セキュリティ管理領域５０内に留まっているセキュリティコントローラ３をすべて置き忘れと判定するため、車内においてユーザが所持しているセキュリティコントローラ３も置き忘れられたものとみなすこととなる。

【０２２９】

従って、セキュリティ管理対象である車５１が警戒モードに設定されている場合、例えばセキュリティコントローラ３を所持したまま、車内でユーザが仮眠をしていても、このセキュリティコントローラ３を置き忘れとすることができるため、このユーザのセキュリティコントローラ３とセキュリティ管理対象である車５１に近づく正規ユーザ以外の人との組み合わせによって、警戒モードを誤って解除することを防ぐことができる。

【０２３０】

また、本実施の形態に係るセキュリティシステム１では、セキュリティコントローラ３ａ～３ｃすべてがオートセキュリティ機能を利用可能とする構成であった。しかし、複数のセキュリティコントローラ３ａ～３ｃのうちいずれか１台のみをオートセキュリティ機能を有効とする構成であってもよい。

【０２３１】

このように、セキュリティコントローラ３ａ～３ｃが、セキュリティ装置２に登録されている場合であっても、オートセキュリティ機能を有効とするのは、このセキュリティコントローラ３ａ～３ｃのうちのいずれか１つとすることで、置き忘れられたセキュリティコントローラ３によって生じる問題を低減できる。すなわち、置き忘れられたセキュリティコントローラ３と正規ユーザ以外の人の接近によって自動的に設定されている警戒モードが解錠される確率を低くすることができる。

【０２３２】

このオートエキュリティ機能を有効とするセキュリティコントローラ３は、例えば、工場出荷時にオートマスタリモコンとして出荷されたセキュリティコントローラ３のみとしてもよい。あるいは、セキュリティコントローラ３ａ～３ｃのうちユーザによってオートセキュリティ機能を有効とするセキュリティリモコン３を設定されたものとしてもよい。

【０２３３】

前者に比べて後者の方が、セキュリティコントローラ３に対して自由にオートセキュリティ機能を有効な装置とすることができるため、設定の自由度が増すこととなる。

【０２３４】

さらには、オートセキュリティ機能を有効としたいセキュリティコントローラ３から他のセキュリティコントローラ３に対して通信を介してオートセキュリティ機能を有効としないように指示する形態であってもよい。

【０２３５】

また、セキュリティ装置２からオートセキュリティ機能を有効とするセキュリティコントローラ３はどれかという問合せをセキュリティコントローラ３ａ～３ｃそれぞれに通知し、応答があったセキュリティコントローラ３のみをオートセキュリティ機能が有効な装置としてもよい。

【０２３６】

さらには、ユーザが最初あるいは最後に警戒モードへの設定指示等操作を行ったセキュリティコントローラ３をオートセキュリティ機能が有効な装置としてもよい。

【０２３７】

車５１を駐車した際に最初あるいは最後に管理対象である車５１から離れたセキュリティコントローラ３を、オートセキュリティ機能が有効な装置としてもよい。

【０２３８】

なお、セキュリティコントローラ３ａ～３ｃにおいて、いずれか１つだけがオートセキュリティ機能を有効とする場合は、どのセキュリティコントローラ３が、オートセキュリティ機能を有効とするのかについて、セキュリティコントローラ３の通知部４２においてユーザに通知されていることが好ましい。

【０２３９】

なお、本実施形態に係るセキュリティシステム１では、セキュリティコントローラ３は、セキュリティコントローラ３ａ～３ｃという３台であったが、この３台に限定されるものではなく、セキュリティ管理対象のユーザの数に応じて必要なだけ設定することができる。

【０２４０】

また、本実施形態に係るセキュリティシステム１では、セキュリティ管理対象が車５１であったが、このセキュリティ管理対象は車５１に限定されるものではなく、例えば家屋、ビル、オフィス、または金庫などであってもよい。ただし、セキュリティ管理対象が家屋，ビル、オフィス、または金庫などの場合、非警戒モードから警戒モードへの設定変更を行うトリガは、ＡＣＣ電源の「オン」から「オフ」への切替えではなく、ドアや出入口に備えられた警戒モード設定ボタン等をユーザが押すことで実現できる。

【０２４１】

また、上記したセキュリティコントローラ３は、例えば携帯電話と組み合わされたものであってもよい。この場合は、セキュリティ装置２は、ＧＰＳによる位置情報を利用できるため、より正確なセキュリティコントローラ３の位置を把握することができる。

【産業上の利用可能性】

【０２４２】

セキュリティ装置２は、セキュリティコントローラ３を所持しない人の接近または侵入等に対して威嚇行為および通知を行うことができるため、特定の権限を有する人以外の利用を制限することが好ましい領域における監視にも適用できる。

【図面の簡単な説明】

【０２４３】

【図１】本発明の実施形態を示すものであり、セキュリティ装置の概略構成の一例を示すブロック図である。

【図２】セキュリティ管理領域における、セキュリティコントローラ３を携帯した人と、セキュリティコントローラを携帯しない人との関係を示す図である。

【図３】セキュリティ管理対象である車を含むセキュリティ管理領域における、セキュリティコントローラ３を携帯した人（ユーザ）と、セキュリティコントローラ３を携帯しない人との関係を示す図である。

【図４】本実施の形態に係るセキュリティシステムの概略構成の一例を示すブロック図である。

【図５】本実施の形態に係るセキュリティ監視テーブルに記録される情報の一例を示す図である。

【図６】本実施の形態に係るセキュリティコントローラの概略構成の一例を示すブロック図である。

【図７】本実施の形態に係るセキュリティ装置における警戒待ち処理の一例を示すフローチャートである。

【図８】本実施形態の比較例としてのセキュリティ装置における警戒待ち処理の一例を示すフローチャートである。

【図９】本実施の形態に係るセキュリティ装置における警戒処理および警戒処理解除の一例を示すフローチャートである。

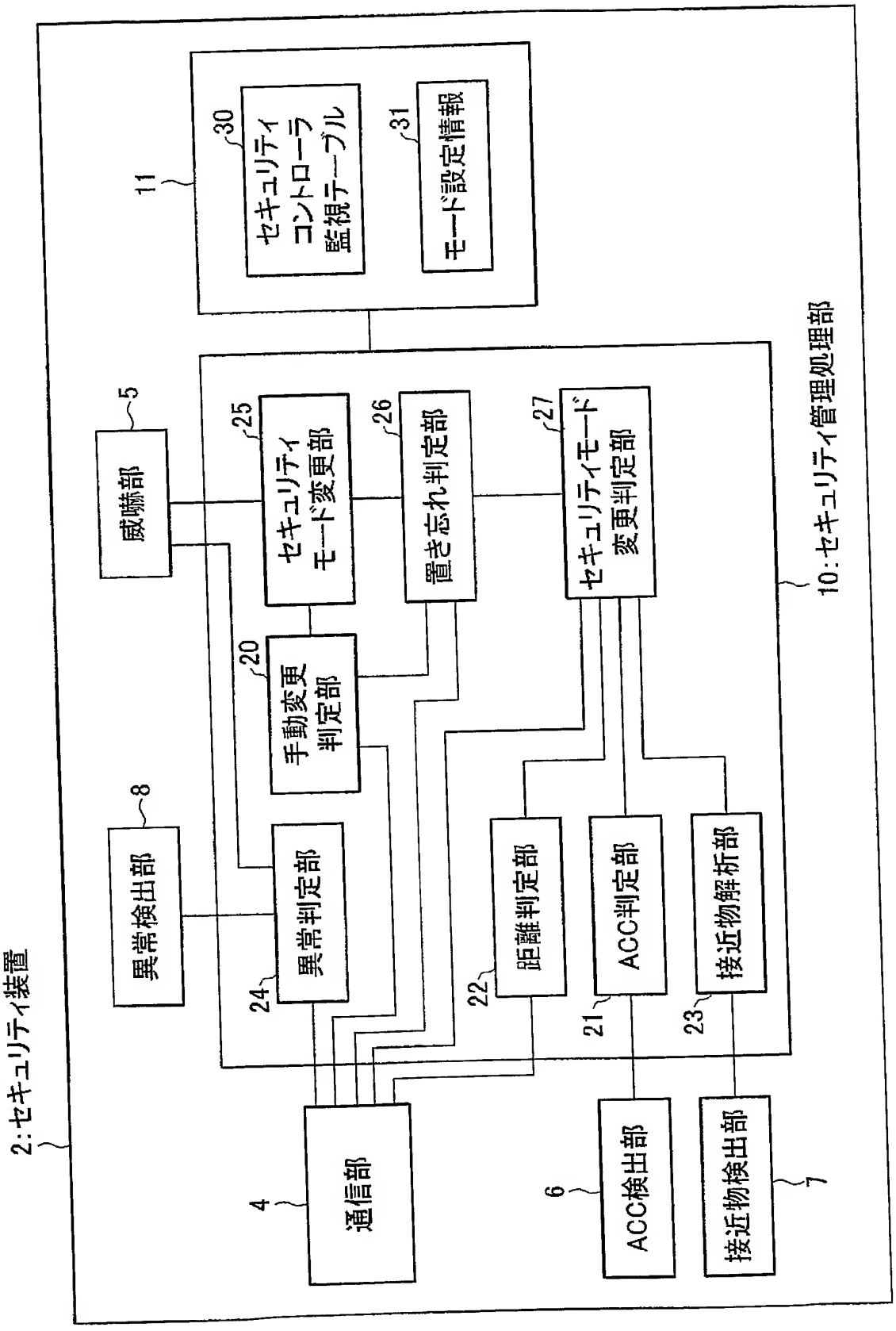
【図１０】本実施形態の比較例としてのセキュリティ装置における警戒処理および警戒処理解除の一例を示すフローチャートである。

【符号の説明】

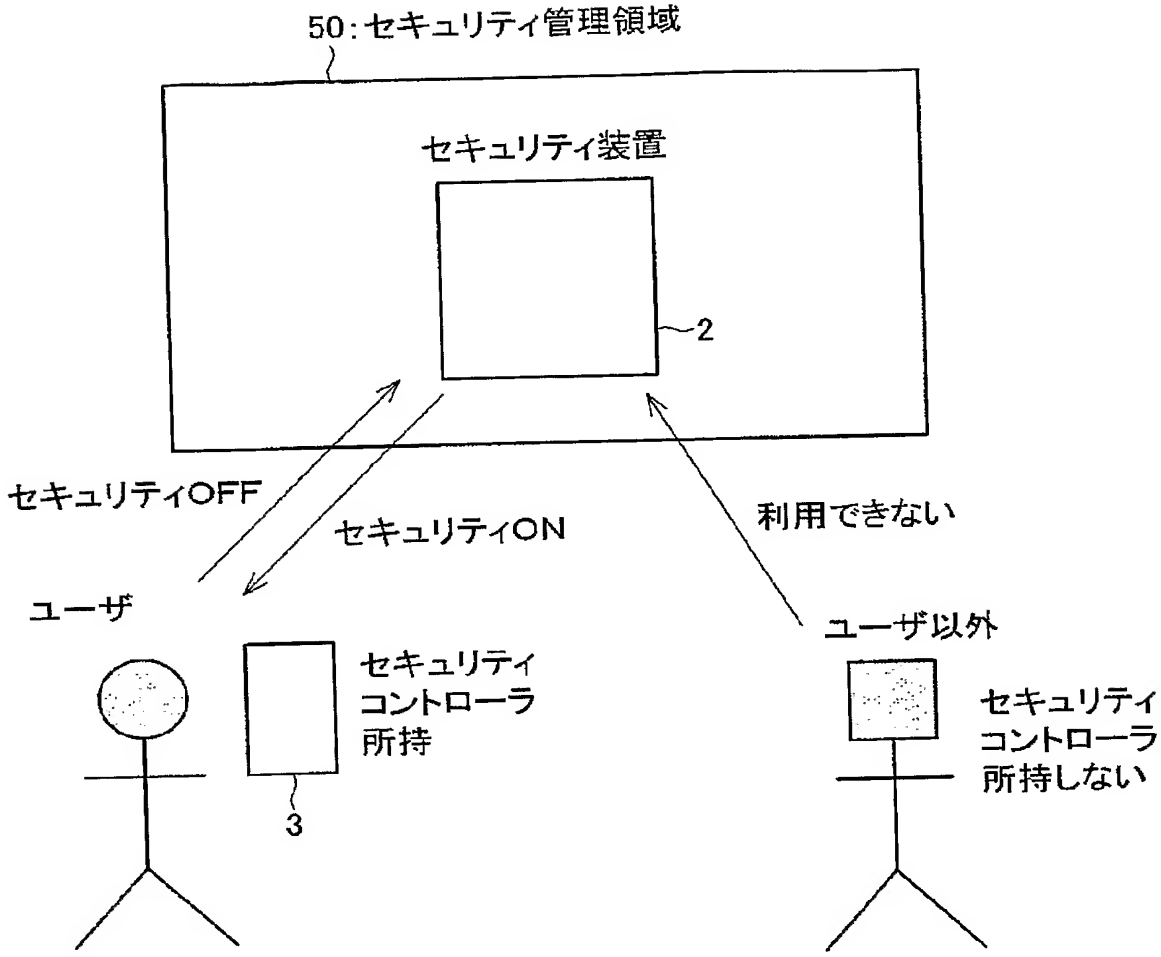
【０２４４】

１　セキュリティシステム（情報処理制御システム）
２　セキュリティ装置（情報処理装置）
３　セキュリティコントローラ（情報送受信装置）
４　通信部（通信装置、位置認識装置）
６　異常検出部
７　接近物検出部（人行動監視手段）
１０　セキュリティ管理処理部
１１　記憶部（履歴記憶装置）
２０　手動変更判定部（第２警戒指示手段）
２２　距離判定部（位置判定手段）
２３　接近物解析部（人行動監視手段）
２４　セキュリティモード変更判定部（第１警戒指示手段）
２６　置き忘れ判定部(警戒状態選択手段、応答要求手段)
２５　セキュリティモード変更部
３０　セキュリティコントローラ監視テーブル（位置履歴情報）
５０　セキュリティ管理領域（所定領域）

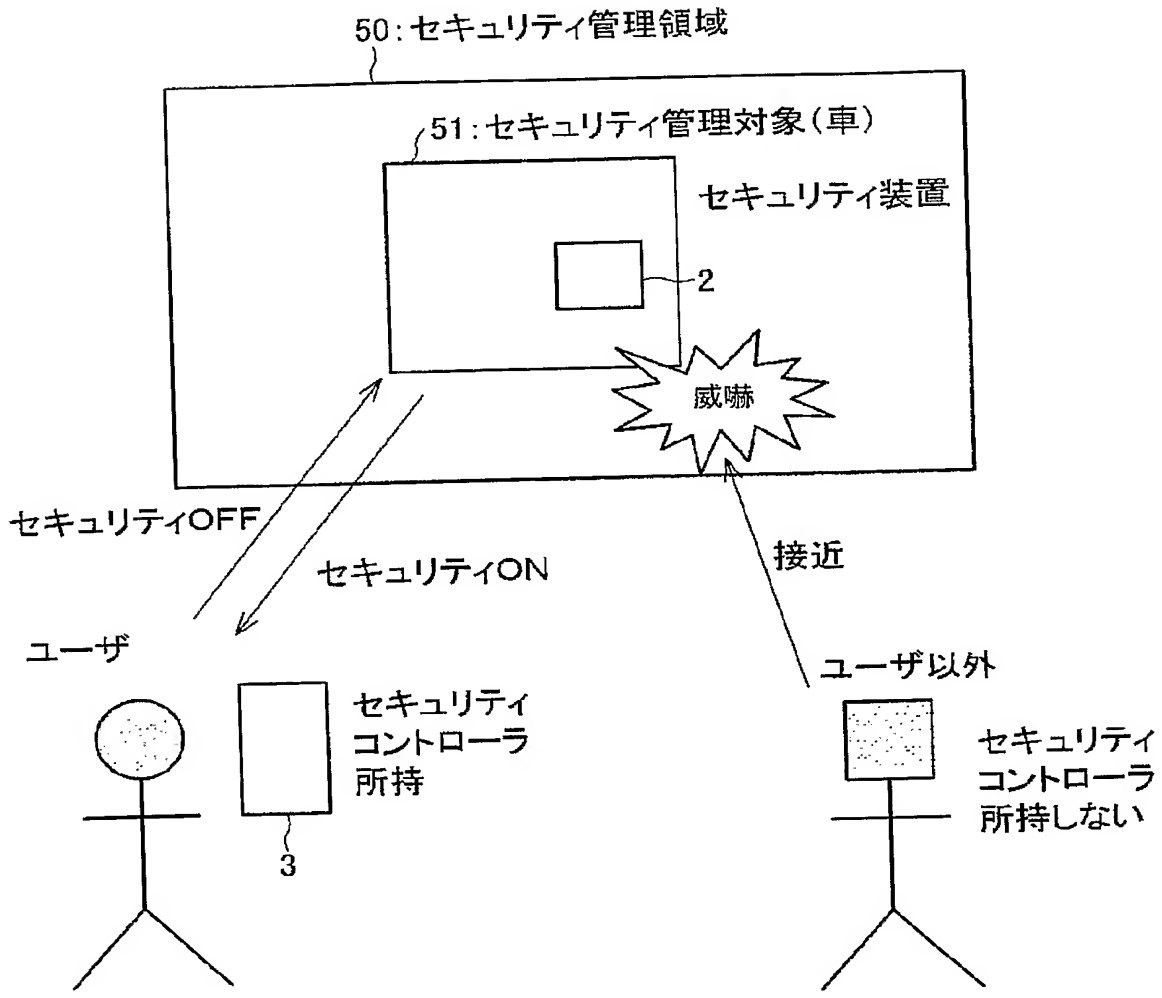
【書類名】図面
【図１】


2:セキュリティ装置
10:セキュリティ管理処理部
11
30
セキュリティ
コントローラ
監視テーブル
31
モード設定情報
5
威嚇部
25
セキュリティ
モード変更部
26
置き忘れ判定部
27
セキュリティモード
変更判定部
20
手動変更
判定部
8
異常検出部
24
異常判定部
22
距離判定部
21
ACC判定部
23
接近物解析部
4
通信部
6
ACC検出部
7
接近物検出部

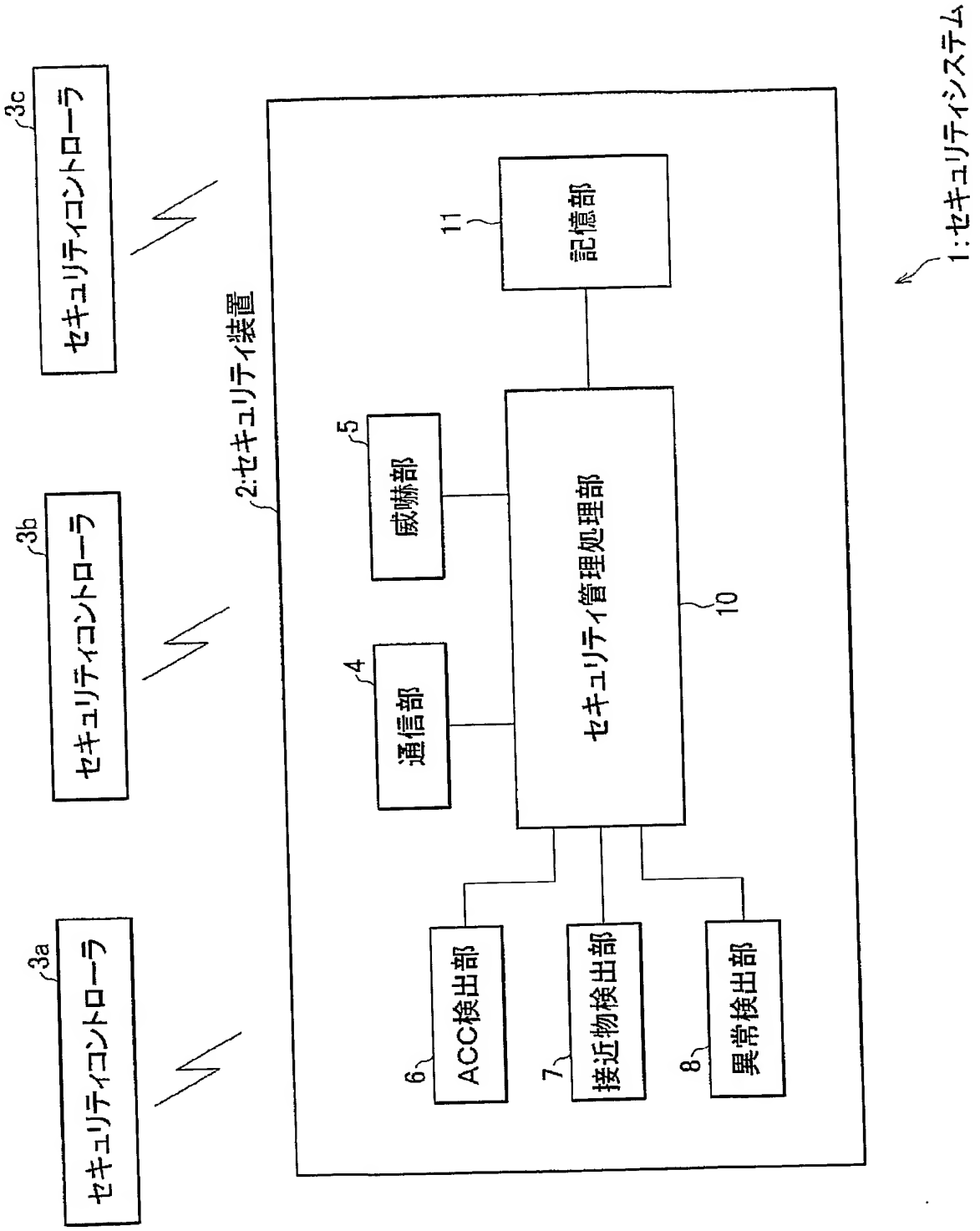
【図２】


50:セキュリティ管理領域
セキュリティ装置
2
セキュリティOFF
セキュリティON
利用できない
ユーザ
セキュリティ
コントローラ
所持
3
ユーザ以外
セキュリティ
コントローラ
所持しない

【図３】


50：セキュリティ管理領域
51：セキュリティ管理対象（車）
セキュリティ装置
2
威嚇
セキュリティOFF
セキュリティON
接近
ユーザ
セキュリティ
コントローラ
所持
3
ユーザ以外
セキュリティ
コントローラ
所持しない

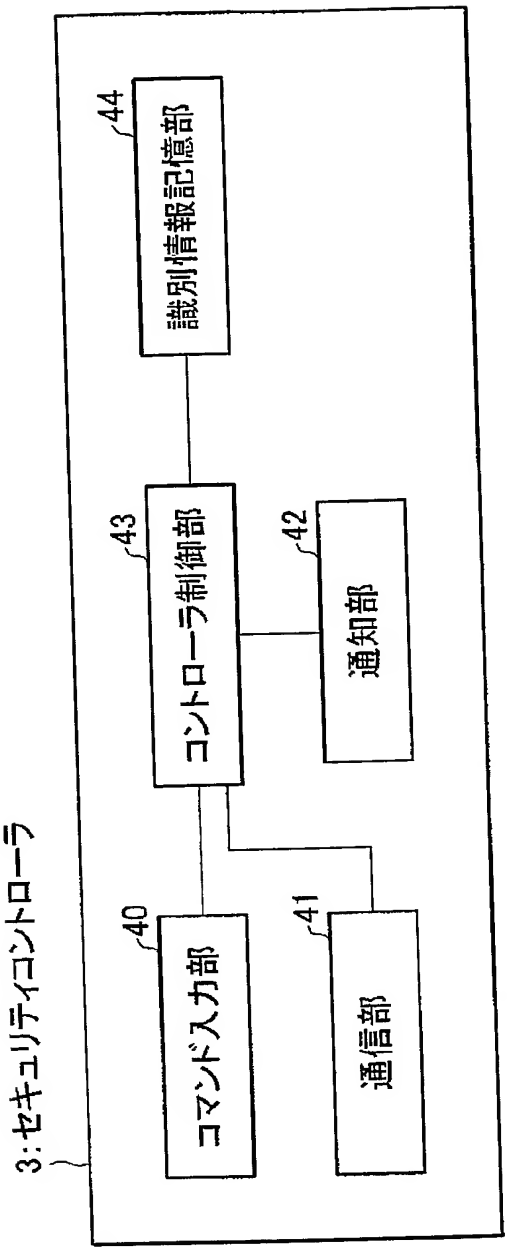
【図４】


1:セキュリティシステム
2:セキュリティ装置
3a
セキュリティコントローラ
3b
セキュリティコントローラ
3c
セキュリティコントローラ
4
通信部
5
威嚇部
6
ACC検出部
7
接近物検出部
8
異常検出部
10
セキュリティ管理処理部
11
記憶部

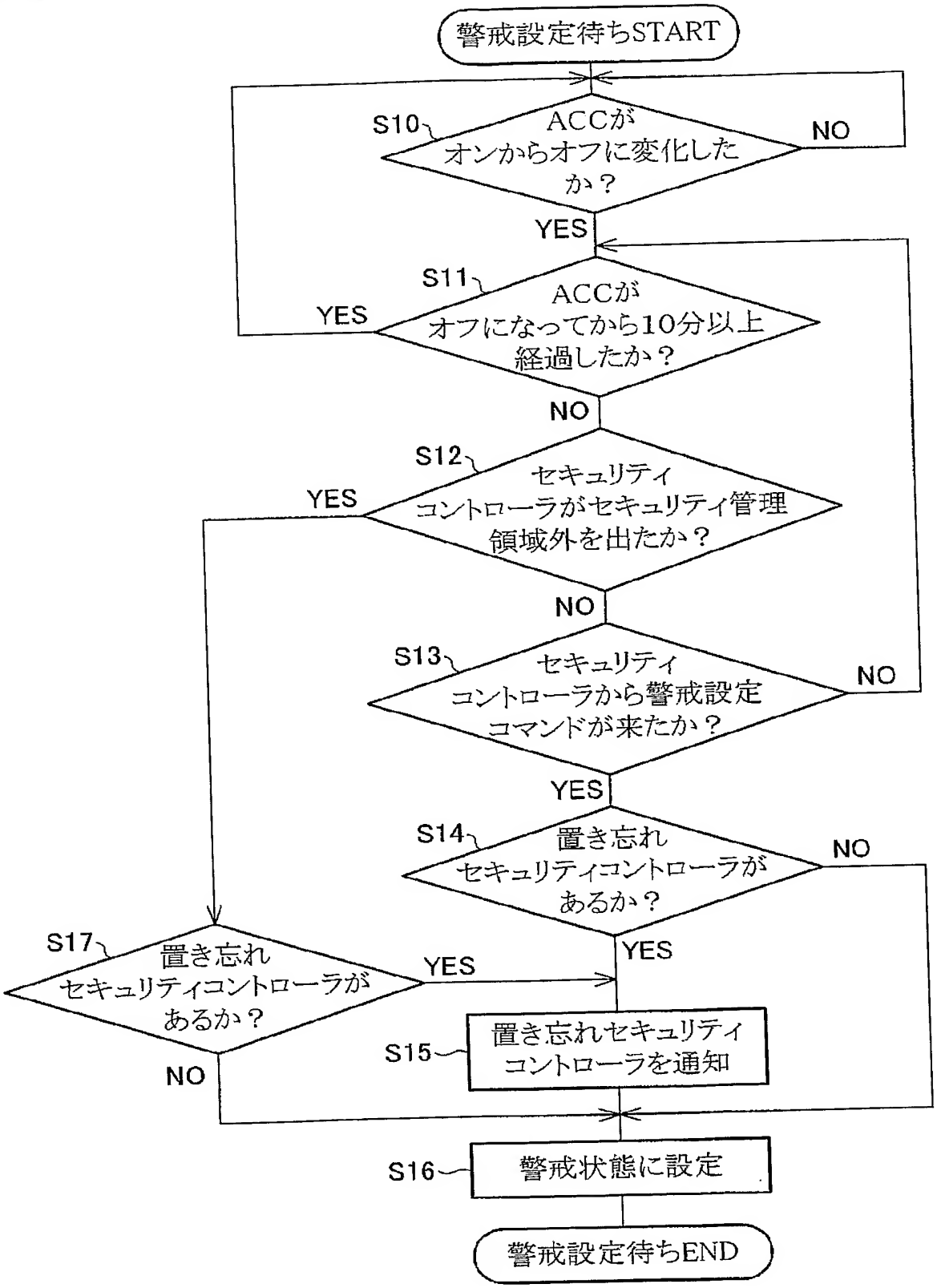
【図５】

セキュリティコントローラ ＼ 時間	0:00（現在）	0:20
セキュリティコントローラ3a	電波強度3．5	電波強度2．0
セキュリティコントローラ3b	電波強度3	電波強度2．3
セキュリティコントローラ3c	電波強度10	電波強度10

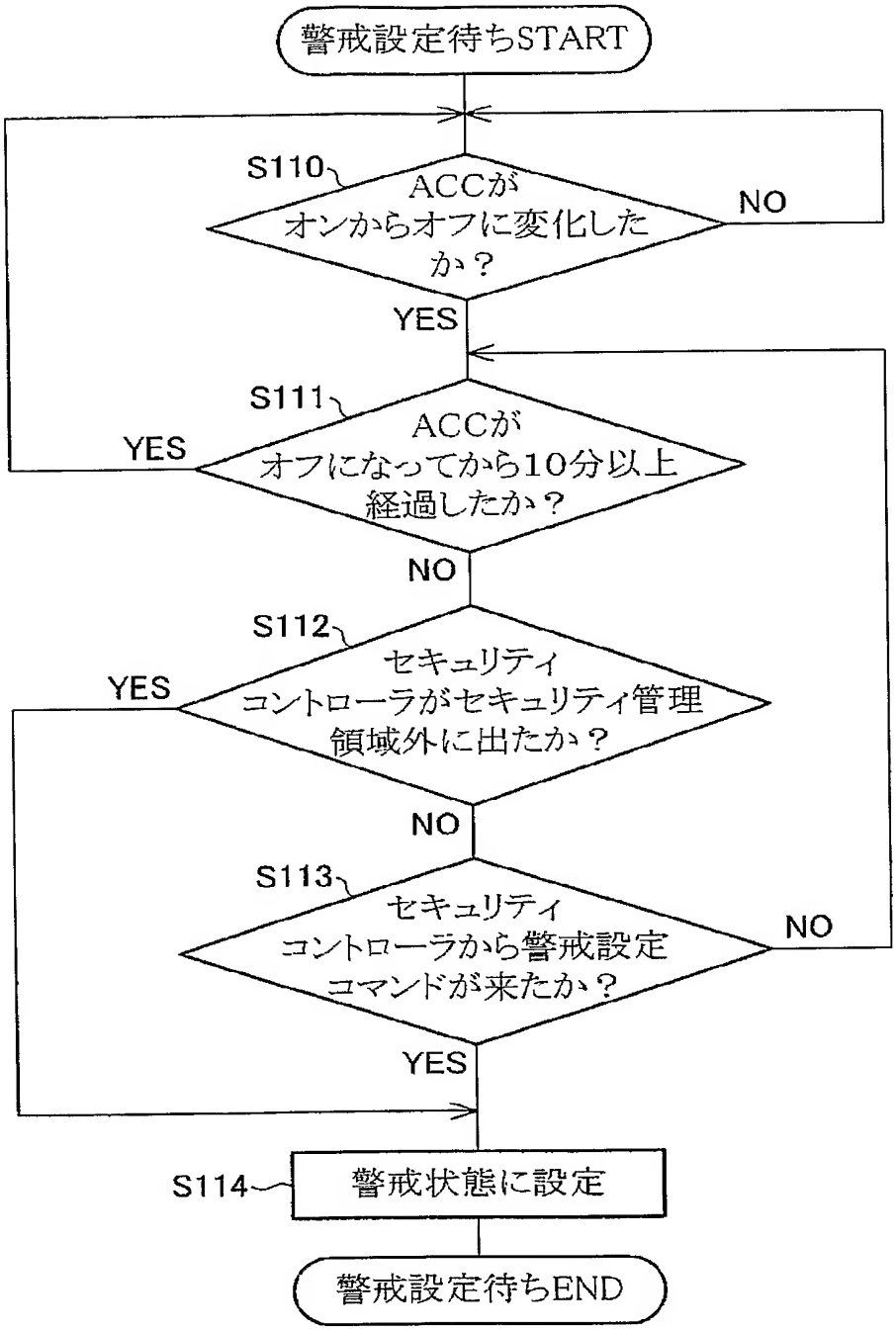
【図６】


3:セキュリティコントローラ
40
コマンド入力部
41
通信部
43
コントローラ制御部
42
通知部
44
識別情報記憶部

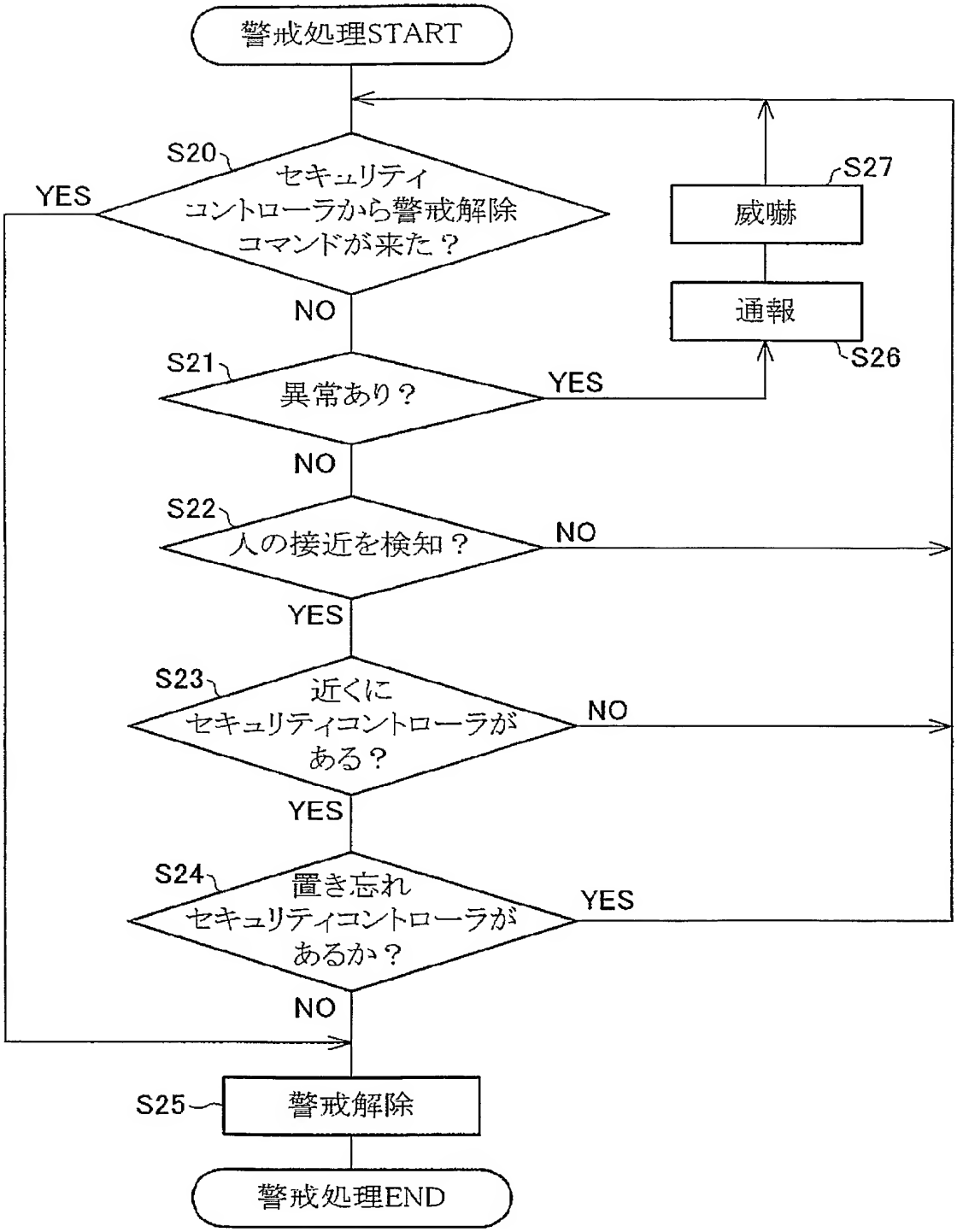
【図７】


警戒設定待ちSTART
S10
ACCがオンからオフに変化したか？
NO
YES
S11
ACCがオフになってから10分以上経過したか？
YES
NO
S12
セキュリティコントローラがセキュリティ管理領域外を出たか？
YES
NO
S13
セキュリティコントローラから警戒設定コマンドが来たか？
NO
YES
S14
置き忘れセキュリティコントローラがあるか？
NO
YES
S17
置き忘れセキュリティコントローラがあるか？
YES
NO
S15
置き忘れセキュリティコントローラを通知
S16
警戒状態に設定
警戒設定待ちEND

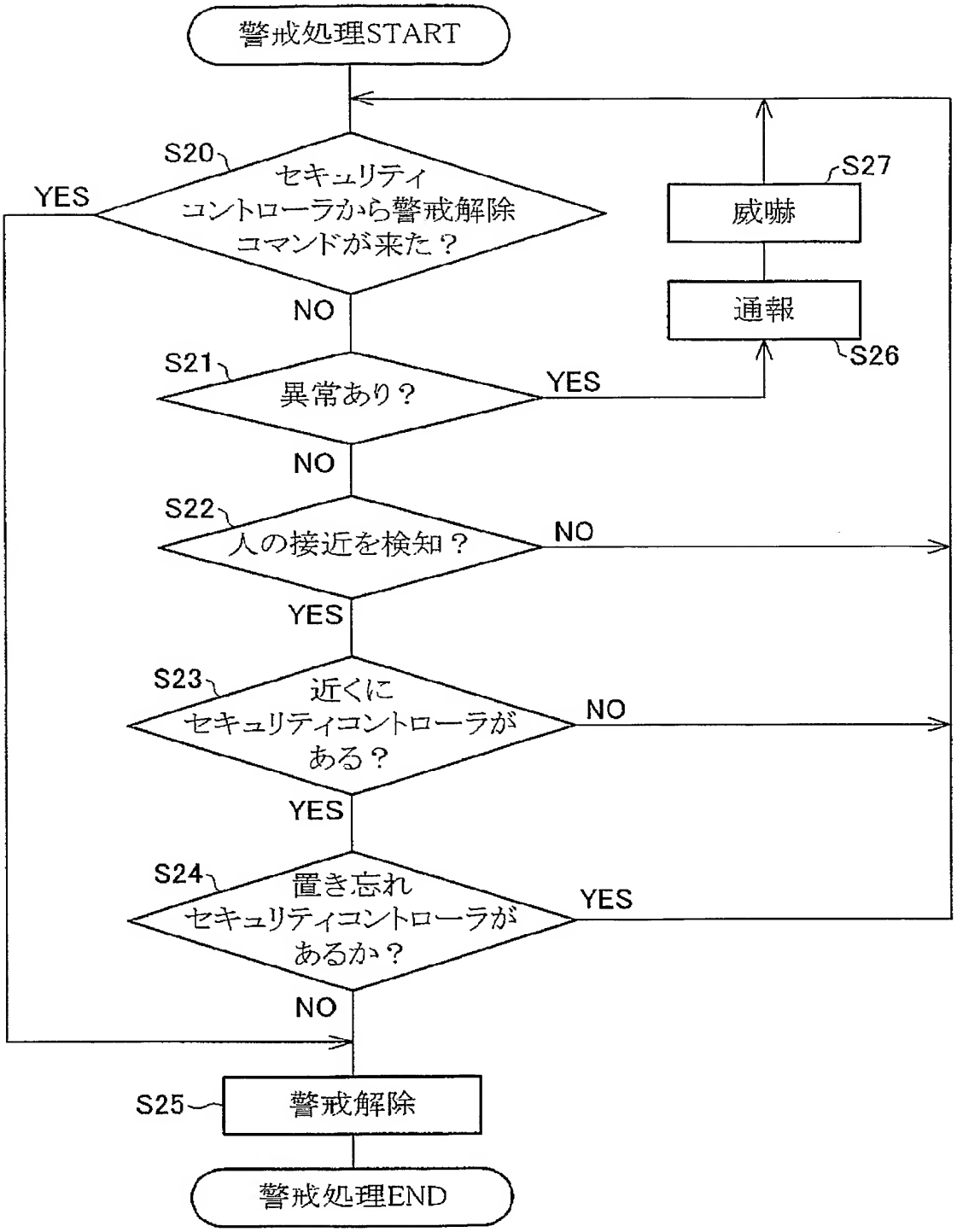
【図８】


警戒設定待ちSTART
S110
ACCが
オンからオフに変化した
か？
NO
YES
S111
ACCが
オフになってから10分以上
経過したか？
YES
NO
S112
セキュリティ
コントローラがセキュリティ管理
領域外に出たか？
YES
NO
S113
セキュリティ
コントローラから警戒設定
コマンドが来たか？
NO
YES
S114
警戒状態に設定
警戒設定待ちEND

【図９】


警戒処理START
S20
セキュリティ
コントローラから警戒解除
コマンドが来た？
YES
NO
S21
異常あり？
YES
S27
威嚇
通報
S26
NO
S22
人の接近を検知？
NO
YES
S23
近くに
セキュリティコントローラが
ある？
NO
YES
S24
置き忘れ
セキュリティコントローラが
あるか？
YES
NO
S25
警戒解除
警戒処理END

【図１０】


警戒処理START
S20
セキュリティ
コントローラから警戒解除
コマンドが来た？
YES
NO
S21
異常あり？
YES
S27
威嚇
通報
S26
NO
S22
人の接近を検知？
NO
YES
S23
近くに
セキュリティコントローラが
ある？
NO
YES
S24
置き忘れ
セキュリティコントローラが
あるか？
YES
NO
S25
警戒解除
警戒処理END

【書類名】要約書
【要約】
【課題】　複数の情報送受信装置が情報処理装置に登録されている場合、当該複数の情報送受信装置の置き忘れによって生じる警戒状態の設定の誤操作を解消することを実現する情報処理装置を提供する。
【解決手段】　セキュリティ装置２は、セキュリティコントローラ３ａ～３ｃを所持したユーザのセキュリティ管理領域５０に対する出入りを監視し、警戒動作の制御を行う。このセキュリティ装置２は、セキュリティコントローラ３ａ～３ｃそれぞれと通信を行い、また、セキュリティコントローラ３ａ～３ｃそれぞれの位置情報を取得する通信部、セキュリティコントローラ監視テーブル３０を記憶する記憶部１１、セキュリティコントローラ３ａ～３ｃが所定領域内に置き忘れられたものであるか否かを判定し、自動的に警戒状態の設定または解除を指示するのか、ユーザの操作入力によって警戒状態の設定または解除を指示するのかを判定する置き忘れ判定部２６を備える。
【選択図】　図１

特願２００４－１０６９４６

出　願　人　履　歴　情　報

識別番号　［０００００２９４５］

１．変更年月日　２０００年　８月１１日
［変更理由］　住所変更
住　所　京都市下京区塩小路通堀川東入南不動堂町８０１番地
氏　名　オムロン株式会社